5-2018

Tactics, Techniques and Procedures (TTPs) to Augment Cyber Threat Intelligence (CTI): A Comprehensive Study

Mohammad Ashraful Huq Shahi
St. Cloud State University, ahshahi@gmail.com

Tactics, Techniques and Procedures (TTPs) to Augment Cyber Threat Intelligence (CTI): A Comprehensive Study

by

Mohammad Ashraful Huq Shahi

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science in

Information Assurance

May, 2018

Starred Paper Committee:
Tirthankar Ghosh, Chairperson
Dennis C. Guster
Jim Q. Chen

Abstract

Sharing Threat Intelligence is now one of the biggest trends in cyber security industry. Today, no one can deny the necessity for information sharing to fight the cyber battle. The massive production of raw and redundant data coupled with the increasingly innovative attack vectors of the perpetrators demands an ecosystem to scrutinize the information, detect and react to take a defensive stance. Having enough sources for threat intelligence or having too many security tools are the least of our problems. The main challenge lies in threat knowledge management, interoperability between different security tools and then converting these filtered data into actionable items across multiple devices. Large datasets may help filtering the massive information gathering, open standards may somewhat facilitate the interoperability issues, and machine learning may partly aid the learning of malicious traits and features of attack, but how do we coordinate the actionable responses across devices, networks, and other ecosystems to be proactive rather than reactive? This paper presents a study of current threat intelligence landscape (Tactic), information sources, basic Indicators of Compromise (IOCs) (Technique) and STIX and TAXII standard as open source frameworks (Procedure) to augment Cyber Threat Intelligence (CTI) sharing.

Acknowledgements

I would like to express my very great appreciation to my culminating project committee members Dr. Tirthankar Ghosh, Dr. Dennis C. Guster and Dr. Jim Q. Chen for their time and cooperation. Special thanks go to Dr. Tirthankar Ghosh for his valuable and constructive suggestions during the planning and development of this paper, and assistance in keeping progress on schedule. His willingness to give his time so generously has been very much appreciated.

I would also like to express my deep gratitude to my family and colleagues for their understanding and patience during my stressful times, also for their enthusiastic encouragement, and useful critiques of this paper work. My grateful thanks are also extended to Mr. Hasib Ahsan Nadeem for his suggestions in developing a methodology for information collection and analysis for this paper.

Finally, I want to thank my parents for being there as my cheerleaders in life and their blessings, support, and inspiration throughout my study.

“Threat is a mirror of security gaps. Cyber-threat is mainly the reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience.”

— Stephane Nappo

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Introduction

Is every penny spent for securing the business actually helping? A question every concerned decision maker would ask to judge the value of their investment. While comparing with the increasing capabilities of the perpetrators both in skillset and innovativeness, often the Security Operation Center (SOC) team falls behind. They are left with analyzing how it happened, learn what was leveraged and try to be proactive for the future. This is where Threat Intelligence also known as Cyber Threat Intelligence (CTI) comes into play to bridge gaps. CTI can be defined in a lot of ways, but the most cited definition is from McMillan (2013) of Gartner, “Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.” SANS Institute simplified their definition as, “The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators.”

Threat Intelligence (TI) sounds great in theory, but its full advantage can be utilized by integrating this knowledge into security operations to augment and automate threat detection capability. Threats come from internal and/or external sources, and the most painful and time-consuming task is to analyze this abundant incoming unstructured raw data to extract meaningful information that is useful enough to take informed decisions or action. In an award-winning research, marketing and publishing

firm CyberEdge LLC, in their 2017 cyber defense survey report, shows exactly why organizations are integrating commercial and/or open source CTI into their existing security infrastructure (see Figure 1) (CyberEdge, 2017). The incremental gains of the CTI use cases suggest that SOC teams are growing in intelligence-related practices by utilizing CTI data more thoroughly for longer-term security strategy and investment decisions.

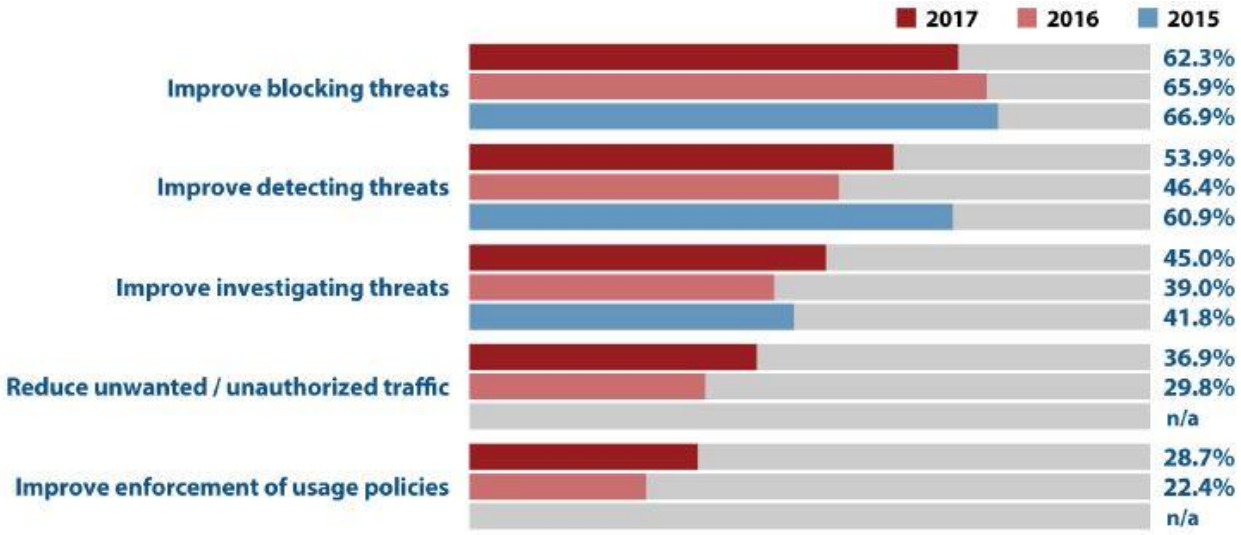


Figure 1: How threat intelligence is being leveraged (CyberEdge, 2017)

Supplemental (i.e., third-party) threat intelligence services continue to be among the hottest areas of investment by organizations seeking to bolster their cyberthreat defenses. But how are IT security teams actually using this valuable resource – which can include everything from ordinary threat indicators (e.g., file hashes and reputation data) and threat data feeds (e.g., malware analysis and trend data) to strategic

intelligence (e.g., detailed information on adversaries and their motivations, intentions, tactics, techniques, and procedures)? (CyberEdge, 2017)

Traditional methods of blocking bad sites hosting malicious software, and applying patches using commercial security products are not enough to defend against advanced attacks and gain insight on infiltration TTPs. A threat-based defense strategy gains knowledge from analyzing attack incidents and related observables and applies that to stop future attacks from happening. MITRE outlines three elements of a comprehensive threat-based defense as:

1. Cyber threat intelligence analysis.
2. Defensive engagement of the threat.
3. Focused sharing and collaboration.

Figure 2 shows the Cyber Attack Lifecycle (first articulated by Lockheed Martin as the “kill chain”), a framework developed by CTI analysts to better understand the stages of cyberattack. The goal here is to proactively look for indicators of compromise (IOC) and defend while the attack is still on the left side of the kill-chain and before the perpetrator establishes a foothold. McMillan (2013) of Gartner Inc. identified two key challenges of CTI as,

1. Leading indicators of risk to an organization are difficult to identify when the organization’s adversaries, including their thoughts, capabilities, and actions, are unknown.

2. Chief Information Security Officers (CISO) have no direct control over threats to their organizations and can only be aware of the threats and prepared for their arrival.

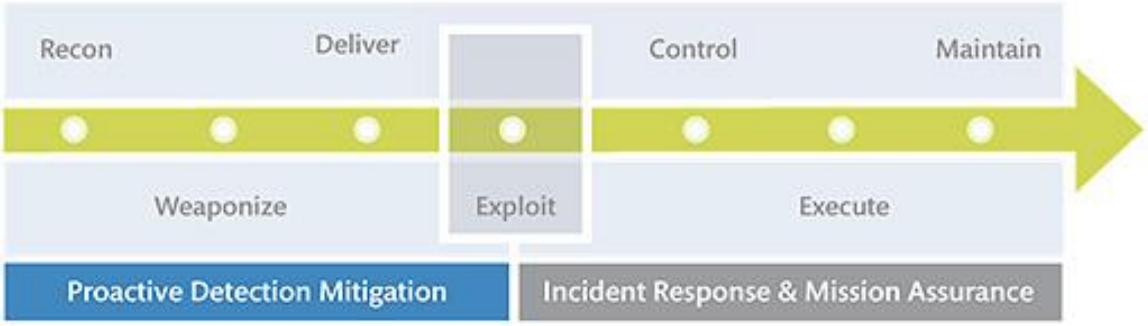


Figure 2: Cyber-attack lifecycle (MITRE, 2017)

It is theorized that all cyber activity can be traced back to the human factor, and as a result the motivations, behavior, and intentions that come with it (St.Clair, 2017). However, to be aware and be prepared for the attack requires collaboration and sharing of IOCs. Several sources and standards have been developed over the years to facilitate CTI sharing, but the problem remains at (1) need for a common language and (2) derive actionable items at all level. Brief descriptions on different CTI tools and standards will be given in the literature review part.

Problem Statement

The full effectiveness of CTI falls short of a seamless threat knowledge management ecosystem, interoperability between different security tools and then converting these filtered data into actionable items across multiple devices. Large datasets may help filtering the massive information gathering, open standards may

somewhat facilitate the interoperability issues and machine learning may partly aid the learning of malicious traits and features of attack, but how do we coordinate the actionable responses across devices, networks, and other ecosystems to proactively respond to threats rather than being reactive to them? This aspect of the problem is the motivation behind this study of Cyber Threat Intelligence (CTI) sources and standards, understand STIX and TAXII as an Expert System and learn how to express IOCs in STIX using JSON. This report may also serve as an initial reference to beginners who wants to explore the world of CTI.

Nature and Significance of the Problem

Several government entities to international consortiums have enacted regulatory compliance guidance e.g. Sarbanes–Oxley Act of 2002 (SOX), Statement on Standards for Attestation Engagements No. 16 (SSAE16), Payment Card Industry Data Security Standard (PCI DSS v3.2) and laws e.g. Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, California Security Breach Information Act (SB-1386) to protect data and privacy. Corporations that allowed breach of consumer data to happen can expect to be sued by the Federal Trade Commission under 15 U.S.C. Sec.45. Nevertheless, lack of proper cyber security defenses may result in major security breach disrupting business capabilities, loss of proprietary corporate data, loss of customer and business partner confidence and costing the organization millions of dollars or more in fines and penalties to federal and state regulatory bodies. Safeguarding the highly relied-upon information systems and data is critical for organizational success.

To be proactive in defending attacks, CTI must be acted upon quickly. The threat landscape is constantly changing, and the effectiveness of CTI largely depends on time. By exchanging cyber-threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through reduction of ambiguity and errors. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread (Johnson, Feldman, Witte and Editors, 2017).

National Institute of Standards and Technology (NIST) is also motivating organizations to take part in sharing CTI information and build trust relationships through its Special Publication (SP) 800-150, Guide to Cyber-Threat Information Sharing (Badger, Johnson, Waltermire, Snyder and Skorupka, 2016).

The study of CTI sources and standards will be helpful for the readers to get up to speed with the topic. And learning about STIX and TAXII will give basic

understanding on how to identify IOCs, interpret in JSON, share via TAXII and contribute observations.

Objective of the Study

The objective of this study is to learn different parts of CTI ecosystem and how this complex structure can be implemented for proactive cyber defense.

The goals of this paper are to (1) study the current CTI landscape to have a quick understanding of relevant tactics and standards available to the security team and an outlook of the CTI sharing architecture; (2) to list major sources of CTI currently used by the SOC teams and basic IOCs that are used to trace incidents including how to interpret the IOCs to a structured machine-parsable human-readable format like JSON in STIX framework; (3) Briefly cover the STIX and TAXII framework to understand how they are used to utilize the full value of CTI and also contribute to the CTI ecosystem with observables.

Limitation of the Study

Since the threat landscape is constantly evolving, the study only includes past and recent publications and tries to analyze and summarize the concepts envisioned in these papers. STIX and TAXII are still under development and going through changes (some major), so examples shown in this paper should not be used in production under any circumstances. Please refer to the respective webpages for further information.

Definition of Terms

Terms	Description
C2	Command and Control stage in Kill-Chain
CAPEC	Common Attack Pattern Enumeration and Classification is a community-driven software security effort to create publicly available catalog of attack patterns.
CCE	Common Configuration Enumeration provides unique identifiers to system configuration issues in order to facilitate correlation of configuration data across multiple information sources and tools.
CEE	Common Event Expression improves the audit process and the ability of users to effectively interpret and analyze event log and audit data.
CIF	Collective Intelligence Framework is a cyber threat intelligence management system.
CISO	Chief Information Security Officer is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.
CPE	Common Platform Enumeration is a structured naming scheme for information technology systems, software, and packages.
CPNI	Centre for the Protection of National Infrastructure is the United Kingdom government authority which provides protective security advice to businesses and organizations across the national infrastructure.
CVE	Common Vulnerabilities and Exposures is a list of common identifiers for publicly known cyber security vulnerabilities.
CVRF	Common Vulnerability Reporting Framework is an XML-based language that enables cross organization sharing of critical security-related information in a single format.
CVSS	Common Vulnerability Scoring System is a standard way to measure vulnerability severity rating
CWE	Common Weakness Enumeration is a community-developed list of common software security weaknesses.
CWSS	The Common Weakness Scoring System provides a mechanism for prioritizing software weaknesses in a consistent, and open manner.
DFP	Data Feed Provider is a software instance that acts as a producer of STIX 2.0 content.
FIRST	FIRST is the global Forum of Incident Response and Security Teams.
HIPAA	Health Insurance Portability and Accountability Act of 1996 is a United States legislation that provides data privacy and security provisions for safeguarding medical information
HITECH	Subtitle D of Health Information Technology for Economic and Clinical Health Act addresses the privacy and security concerns associated with the electronic transmission of health information.
IDMEF	Intrusion Detection Message Exchange Format defines data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them.

Terms	Description
IDS, NIDS, HIDS	An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.
IOC	Indicator of Compromise
IODEF	Incident Object Description Exchange Format defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams about computer security incidents.
IPS, NIPS, HIPS	An Intrusion Prevention System is a network security threat prevention technology that examines network or system traffic flows to detect and prevent vulnerability exploits.
JANER-CERT	Joint Academic NETwork Computer Emergency Response Team
JSON	JavaScript Object Notation is a lightweight data-interchange format.
MITRE	MITRE is a not-for-profit organization that operates research and development centers sponsored by the federal government.
NIST	The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce promoting innovation and industrial competitiveness.
OASIS	Organization for the Advancement of Structured Information Standards is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.
OPENIOC	A standard for recording, defining and sharing information both internally and externally in a machine-readable format
OSSIM	Open Source Security Information and event Management system integrates a selection of tools designed to aid network administrators in computer security, intrusion detection and prevention.
OTX	Open Threat Exchange is the world's largest crowd-sourced computer-security platform.
OVAL	Open Vulnerability and Assessment Language is an information security community effort to standardize how to assess and report upon the machine state of computer systems.
PCI DSS	Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.
REN-ISAC	Research & Education Networking Information Sharing & Analysis Centers aids and promotes cybersecurity operational protection and response within the research and higher education communities.
RESTFUL API	An application program interface (API) that uses HTTP requests to GET, PUT, POST and DELETE data.
RID	Real-time Inter-Network Defense outlines a proactive inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution.
SANS	SANS Institute is a private U.S. for-profit company that specializes in information security and cybersecurity training.

Terms	Description
SIEM	Security information and event management technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources.
SOC	Security Operations Center is a centralized unit that deals with security issues on an organizational and technical level.
SOX	Sarbanes–Oxley Act of 2002 protects investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.
SSAE16	Statement on Standards for Attestation Engagements 16 is an auditing standard for service organizations
STIX	Structured Threat Information Expression is a structured language for cyber threat intelligence
TAXII	Trusted Automated Exchange of Intelligence Information is a transport mechanism for sharing cyber threat intelligence
TDS	Threat Detection System is a software instance of any network product that monitors and/or detects such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc.
TIP	Threat Intelligence Platform is a software instance that aggregate correlate and refine threat data from multiple sources in real time and share intelligence with other machines or security personnel operating in security infrastructure.
TLP	The Traffic Light Protocol is a set of designations used to ensure that sensitive information is shared with the appropriate audience.
TMS	Threat Mitigation System is a software instance that acts on course of actions and other threat mitigations such as a firewall or IPS, Endpoint Detection and Response (EDR) software, etc.
URI / URL	Uniform Resource Identifier is a string of characters used to identify a resource. Uniform Resource Locator is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
US-CERT	The United States Computer Emergency Readiness Team is an organization within the Department of Homeland Security's National Protection and Programs Directorate.
VERIS	Vocabulary for Event Recording and Incident Sharing is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner.
XCCDF	Extensible Configuration Checklist Description Format is a structured collection of security configuration rules for some set of target systems.

Summary

For a business to be successful in the current technology era, decision makers need to make informed, long term decisions and invest in intelligence-related practices more backed by the right skills and technology to proactively defend their assets. Leveraging the full potential of supplemental CTI services as a sharing community is the smart move now, but it also requires active contribution and feedback from the trust groups to improve quality of CTI. A threat-based defense strategy is the core of CTI ecosystem and gives the cyber defenders a change to be proactive rather than reactive in the kill-chain. Coordination of IOCs, CTI and actionable responses, tracing back cyber activities to the human factor and blocking them in response is possible. Regulations and laws are guidelines only and may impose compliance restrictions on organizations, but the perpetrators roam freely and are very skilled. Fighting this battle requires teamwork, vigilance, and quick actions against threats which is only possible when CTI is empowered by more active members from the community. This chapter gives the readers an insight of the importance of CTI ecosystem and identifies the motivation of this paper and study goals. The next chapter will discuss the current CTI landscape, existing standards, CTI sources and more about the STIX and TAXII standards.

Chapter II: Background and Review of Literature

Introduction

WannaCry in May 2017, and then NotPetya in June 2017, are just two examples of ransomware attacks amongst others spreading into industries across the world making the cyber landscape ever more threatening day by day. It is surprising to see how organizations are still reluctant to allocate budgets for CTI driven security which is crucial to their cyber defense. The 2016 SANS report (Shackleford, 2016) addresses this problem and notes, “The [threat intelligence] landscape today is very fragmented, and there are few consistent themes in terms of approaches organizations are taking: lots of tools, lots of ‘standards’ and little agreement on which are best may lead to more confusion. For the future, organizations must be able to use tools and CTI data in a more integrated way.” Figure 3 (Athias, 2015) shows the contributing bodies to current CTI ecosystem.

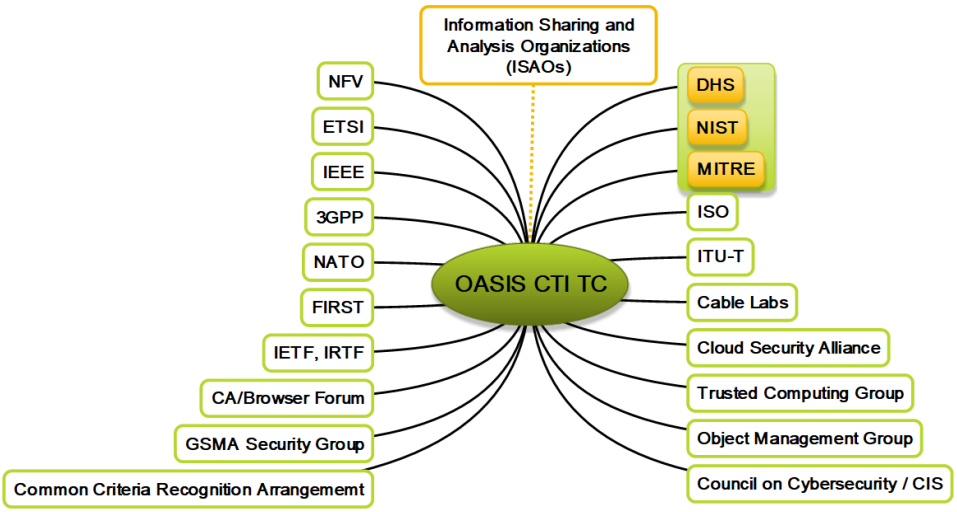


Figure 3: CTI ecosystem (Athias, 2015)

OASIS (known as SGML Open prior to 1993) Cyber Threat Intelligence (CTI) Technical Committee is a non-profit consortium representing 5,000 participants from 600 organizations and individual members from 65 countries driving the development, convergence, and adoption of open standards for the global information society. OASIS is distinguished by its transparent governance and operating procedures. In addition to the organizations listed in Figure 3, Boeing, Check Point, Cisco, Dell, HP, Intel Security, Microsoft, EMC, Fujitsu, IBM, iboss, iSIGHT Partners, NEC, New Context, BrightPoint Security, Tripwire, Palo Alto Networks, Splunk, Resilient, Securonix, Soltra, TELUS, ThreatQuotient, ThreatStream, TruSTAR, ViaSat, and many more are collaborating to develop the foundational cyber security specifications, STIX, CybOX (now merged with STIX 2.0), TAXII with OASIS CTI TC (oasis-open website). A detailed list of supporters can also be found at https://wiki.oasis-open.org/cti/Products (Products) and https://wiki.oasis-open.org/cti/Open%20Source%20Projects (Open Source Projects).

How to Approach CTI

CTI approaches can be looked at from different angles. Farnham (2013) showed how CTI can be utilized from a Project Management Body of Knowledge (PMBOK) perspective taking leverage of its standard processes and deliverables for project management in his fictitious project. However, a more classical approach was well explained by Poputa-Clean (2015) in his paper regarding automated defense by looking at CTI from Strategic Intelligence vs Tactical Intelligence perspective. A third approach can be derived from Farnham's (2013) paper that works with trust groups focusing on specific objectives using relevant tools and standards for ease of sharing CTI data.

While the project management approach is useful for complex CTI projects, and trust groups have CTI data sharing agreement between them, the classical approach is more relevant in terms, and understandable to the business decision makers.

Strategic Intelligence requires more high-level human analysis as it focuses on profiling threat actors (such as criminal profiling in CIA, FBI) utilizing CTI of their trend, TTPs, targets and tools preferred. Tactical Intelligence is more quantifiable (e.g. IP, hash, file name) and machine-parsable but has a very short lifespan as the adversaries can change them frequently. Poputa-Clean (2015) includes a list of criteria to classify intelligence from Anton Chuvakin's report on "How to Collect, Refine, Utilize and Create Threat Intelligence". The list identifies CTI Gathering methods, Cost of subscription or source, Main usage, Target audience, Specificity or the level of details in the CTI and Lifespan or window of the CTI as the classification criteria. As shown in Table 1, Poputa-Clean (2015) further differentiates between Strategic and Tactical Intelligence from the view point of specificity, type of intelligence, desired outcome, Key performance Indicators.

Table 1: CTI use cases (Poputa-Clean, 2015)

Use Case	Specificity	Strategic/ Tactical	Product	KPI
Security Planning	Low	Strategic	Security Vision, Response Plans, Security Roadmaps	Success in response to targeted attack
Threat Intelligence Collection and Fusion	Low	Both	Threat Intelligence Reports and Indicators	
Incident Response	Medium	Both	Incident Response	Time to containment, correct identification and scoping of incidents
Enterprise Security Monitoring	High	Tactical	Blocks, Alerts, Context	Time to detection, time to escalation, false positive rate for alerts

For the executives, value of CTI has increased over time as they can now relate qualitative CTI data more with their decision-making capabilities. 2016 SANS Cyber Threat Intelligence Survey shows the maturity of CTI programs where 66.4% respondents characterized their CTI programs as maturing and above (see Figure 4) (Shackleford, 2016). This only proves the increasing demand of CTI and that it is now more of a necessity then luxury to the organizations.

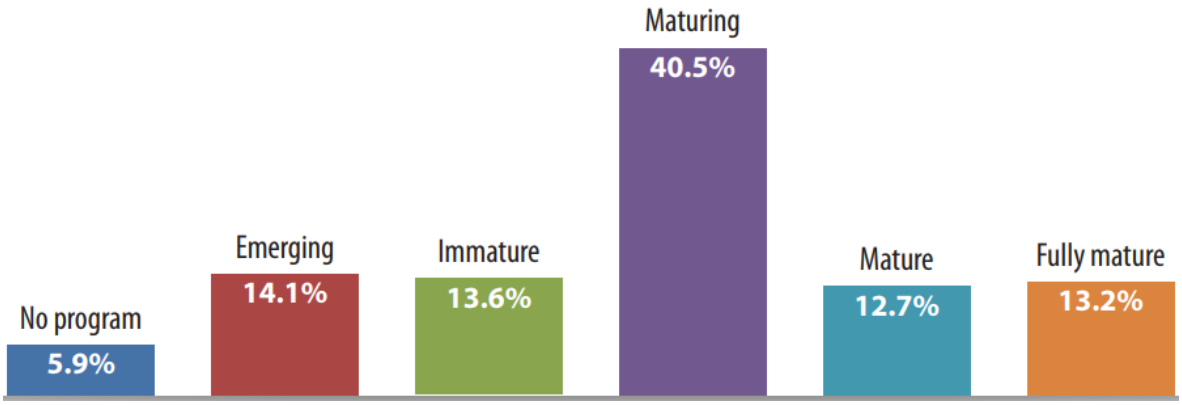


Figure 4: Maturity of CTI programs (Shackleford, 2016)

CTI Sources

CTI sources vary depending on if you are a consumer or producer of CTI. However, Fernham (2013) categorized the main CTI sources as Internal, Community and External.

1. **Internal:** CTI collected from sources internal to the organization such as monitoring tool (e.g. Antivirus, Firewall, IPS, IDS, HIDS, Honeypot) logs, reports and analysis of inbound and outbound data, Computer forensic analysis etc.

2. **Community:** CTI shared through trusted relationships such as informal groups with member organizations or formal groups.
3. **External:** CTI collected through public sources (Open source, books, publications, Internet, Crowdsourced platforms) and private sources (Paid subscriptions, regular threat feeds from a vendor, purchased services).

Veerasamy (2017) had a slightly different view of the sources. He quotes the three sources of CTI as Signal Intelligence (SIGINT) that consists of CTI data from inception and analysis of network data to identify anomalies, Open Source Intelligence (OSINT) that contains CTI data that is publicly available through internet, publications or crawling technologies to produce good quality CTI and lastly, Human Intelligence (HUMINT) that depends on human analysis and research on collected CTI data using automated software to detect emerging trend and threat actors. Veerasamy's (2017) framework of CTI lists down the sources as,

1. Security community and trusted peers
2. Vendor-driven feeds and subscription services
3. Own data (logs from network, application, system and data)
4. Blacklist websites (bad URL's, phishing sites, C&C sites, botnets, malware)
5. Geographic information about location and source (WHOIS and DNS)
6. Government/ Governmental agencies
7. Crowdsource/Open source data
8. Blogs/online forums
9. Social media

10. CSIRTs
11. Other intelligence organizations

Defining the type of CTI sources help understanding where to look for information but the selection of sources for qualitative and quantitative CTI almost always should follow the below self-directed questions as laid out by Metivier (2016) –

1. Will this information provide us with actionable intelligence that is relevant to our organization's sector, region, and / or infrastructure?
2. Will this information provide us with valuable information to build our long-term knowledge base and strategy?

If the answers to these questions are not known, then it would be a good idea to avoid that source(s). It should be remembered that, actionable CTI is the goal for Tactical Intelligence and CTI that provides long term insight is the goal for Strategic Intelligence. A lot of standards and tools to share these CTI data does give the consumers an option to choose from based on their technology requirements, but it also imposes a problem of not having a common standard that can be integrated seamlessly across tools, devices and platforms. Next, we will explore some of the major CTI sharing standards and tools.

CTI Sharing Standards

The challenges of adopting CTI standards include data privacy, laws governing data sharing, fear of reputation due to disclosing attacks. Despite the challenges, requirements of structured automated sharing of CTI is growing and several organizations including private, public and government have taken major steps to

develop standards that works best. Since, a lot of these standards are still under development a brief overview of few is given below,

1. **Open Indicators of Compromise (OpenIOC) –** introduced in 2011, is an extensible XML schema for the description of technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise. OpenIOC was created by MANDIANT (Farnham, 2013), now a FireEye company, still offering their IOC tools e.g. IOC Editor, IOC Finder, IOC Writer, Redline for free. It is basically used for tactical CTI.
2. **Incident Object Description Exchange Format (IODEF) –** is an XML based structured human readable data format developed by Managed Incident Lightweight Exchange (MILE), an Internet Engineering Task Force (IETF) working group, to describe security incidents for Computer Security Incident Response Team (CSIRT). It is backward compatible and heavily based on Intrusion Detection Message Exchange Format (IDMEF) used for intrusion detection systems. IODEF is supported by tools such as Incident Handling Shell (ihsh), Incident Handling Library (libih), Script from JANER-CERT (XML-IODEF), HP ArcSight. Snort supports IMDEF extensions and plugin (SNML). IODEF Structured Cybersecurity Information (IODEF-SCI) is an extension of IODEF to support additional data classes by embedding existing standards within the IODEF document including attack pattern (CAPEC), vulnerability (CVE, CVRF, CCE), weakness (CWE) as Method and platform ID (CPE), Score (CVSS, CWSS, CCSS), Event Report (CEE), Verification (OVAL,

XCCDF), Remediation (RCE) etc. (NICT-CYBEX Forum). Another standard developed by MILE based of IODEF model is the Real time Inter-network Defense (RID) for communicating CTI which adds Boolean data.

3. **Vocabulary for Event Recording and Incident Sharing (VERIS)** – is a framework from Verizon launched in 2010 that is intended for sharing strategic intelligence data (actors, actions, assets, attributed) and collective view of threat incidents. However, for sharing tactical data it may not be considered as useful (The VERIS Framework). Verizon has a publicly available community database for VERIS data in JASON format.
4. **Traffic Light Protocol (TLP) –** created by the UK Government's National Infrastructure Security Coordination Centre (NISCC, now Centre for Protection of National Infrastructure - CPNI) in the early 2000 (Wikipedia), is a set of labels to categorize the level of sensitive information sharing to proper audience. US Computer Emergency Readiness Team (US-CERT) uses TLP according to the Forum of Incident Response and Security Teams (FIRST) specifications. TLP uses only 4 colors (white, green, amber, red) to label/tag information to indicate expected sharing restrictions. White means ‘Public’, Green means ‘Restricted to the community’, Amber means ‘Restricted to participants’ organizations only’ and Red means ‘Restricted to participants only’. The simplicity of TLP allows it to be incorporated in documents, e-mails or any system.

5. **Open Threat Exchange (OTX)** - is the world's largest crowd-sourced CTI platform with more than 50,000 participants in 140 countries sharing 1m+ potential threats daily and It's free to use. Created by AlienVault in 2012, OTX is technically a cloud-hosted big data platform that integrates natural language processing and machine learning to facilitate the collection and correlation of data from many sources, including third-party threat feeds, websites, OSSIM, external API and local agents. (Wikipedia)
6. **Collective Intelligence Framework (CIF) –** is a CTI management system introduced in 2009 and primarily sponsored by the REN-ISAC community and NSF. CIF can combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route). The most common types of threat intelligence warehoused in CIF are IP addresses, domains and URLs that are observed to be related to malicious activity (CSIRTGadgets). CIF shares threat intelligence through a client/server setup utilizing IODEF as internal storage format and provides feeds or allows searches via CLI and RESTFUL APIs. CIF is capable of exporting CTI for various security tools (Poputa-Clean, 2015).
7. **Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) –** was created by MITRE in 2012 under the patronage of US DHS, currently licensed and governed by the nonprofit consortium OASIS CTI TC. STIX and TAXII are

community-supported specifications intended for automated CTI sharing for real-time network defense, and complex threat analysis. STIX is a fully expressive, flexible, structured, machine parsable, human readable language for CTI. And TAXII like the name suggests is a CTI data transport system (application layer protocol using HTTPS) for STIX with a set of services and message exchanges that enable sharing of actionable threat information across organizations, products, and services (OASIS CTI TC, 2017).

CTI Tool

As mentioned earlier, there are lots of tools for CTI. Though the range of tools varies depending on capability and price, some are still free. Below is a list of some popular tools for CTI with their categories,

1. **Open Source** software such as YARA is developed by VirusTotal and mostly used by malware researchers to identify and classify malware samples. It also lets you create descriptions or rules for malware family-based patterns. This multi-platform tool can be used through its command-line interface or from Python scripts using YARA-Python extension (VirusTotal website).
2. **Security Information and Event Management (SIEM)** software such as ArcSight, Splunk, QRadar, RSA NetWitness are powerful tools that support real time network traffic monitoring allowing incident response of incoming traffic easy to the security team. Known threat signatures can be created with these tools to get instant alerts and deflect threat. SIEM fusion is a well-known term for any security operations team.

3. **CTI Provider Service** tool such as Recorded Future can be integrated with existing security technologies. It provides real-time machine-readable CTI data from numerous threat feeds by adding vital context and IOCs. (Recorded Future website). Hail a TAXII.com is a repository of Open Source Cyber Threat Intelligence feeds in STIX format (HAIL A TAXII website).
4. **Network Traffic Analysis Frameworks** such as SNORT and BRO are also open source. Snort was created by Martin Roesch in 1998, now developed by Sourcefire which is owned by Cisco since 2013. SNORT can do real-time traffic analysis and packet logging on IP networks. It can also perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more (SNORT website). BRO is originally written by Vern Paxson, a UNIX based network monitoring tool that can be used as NIDS or collecting network measurements, conducting forensic investigations, traffic baselining, generating extensive set of log files that records network activity in high level terms and more. BRO can be considered as tcpdump, Snort, netflow and Scripting language (Bro Script) all in one.
5. **Disassembler** such as Interactive Disassembler (IDA) Pro can explore binary program and map a malicious file's execution. It can also debug malware code to reverse engineer, sometimes bypassing obfuscation, making the code more readable.

6. **Web Proxy** tools such as Burp or Burp Suite is a graphical tool for security testing of Web applications. The tool is written in Java and is developed by PortSwigger Security. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a a repeater, a decoder, a comparer, an extender, and a sequencer. (Wikipedia)
7. **Cybersecurity Platforms** such as ThreatConnect is specifically designed to help understanding adversaries, automating workflows, and mitigating threats faster using threat intelligence. It can do indicator analytics, threat intelligence analysis, orchestration, tasking, and more (ThreatConnect website). ENDGAME is another cyber operations platform that supports the detection, exploitation, and mitigation of cyber-threats. ThreatQ CTI platform leverages integrated self-tuning Threat Library, Adaptive Workbench and Open Exchange with robust partner programs to augment security operations. Some other prominent platforms are TruSTAR, BrightPoint Security, NORSE, Webroot (Cloud & AI), Twistlock (Container Security for Docker, Kubernetes and Cloud), LogRhythm (AI & machine Learning), Awesome Threat Intelligence.

"Once an organization has laid the groundwork for a TI implementation by defining it, identifying sources and setting expectations, it must take steps to make TI actionable", (Bromiley, 2016, p. 10). These steps may include but not limited to,

- Incorporating CTI into the organization's security infrastructure

- Using CTI to help drive investigations and response (IOCs and Patterning)
- Using CTI to look into the past and possibly see things that were missed in the absence of the CTI (Host and Network Scanning)
- Using CTI to look into the future (Automate for proactive response)

Indicators of Compromise

Using CTI to help drive investigations and response can be achieved by utilizing information on Indicators of compromise (IOC) and Patterning for contextual information on the course of attack. IOCs are the atomic pieces of artifacts or observable data that can be utilized to detect data breaches quickly. Examples of IOCs are IP addresses of Command and Control (C2) servers, domain names, URLs, registry settings, email addresses, HTTP user agent, file mutex, file hashes, compile times, file size, name, path locations, hash values or similar metadata that may occur during an attack. These IOCs greatly help organizations or network defenders to identify unusual activity on the network or odd clues on systems that may indicate attacker activity and take preventive measures. “By preventing compromise in the first place, the resultant risk is reduced in a way unachievable through the conventional incident response process” (Hutchins, Cloppert and Amin, 2010, p.12).

In the same white paper (Hutchins et al., 2010), the authors also presented tables to show which tools may be utilized to detect, deny, disrupt, degrade, deceive, and destroy the Advanced Persistent Threat (APT) IOCs in the Lockheed Martin’s Kill-Chain phases. See Table 2 which was created by combining table 1 and table 2 from Hutchins et al. (2010 p. 5, 10). However, more than one indicator can be combined to create a

single IOC and not all indicators are equal as some could be more valuable than the others. This is illustrated in Figure 5 (Dittrich and Carpenter, 2016) which was originally created by Mandiant (now, a FireEye company). Table 2 and Figure 5 are of course not showing the same IOC examples.

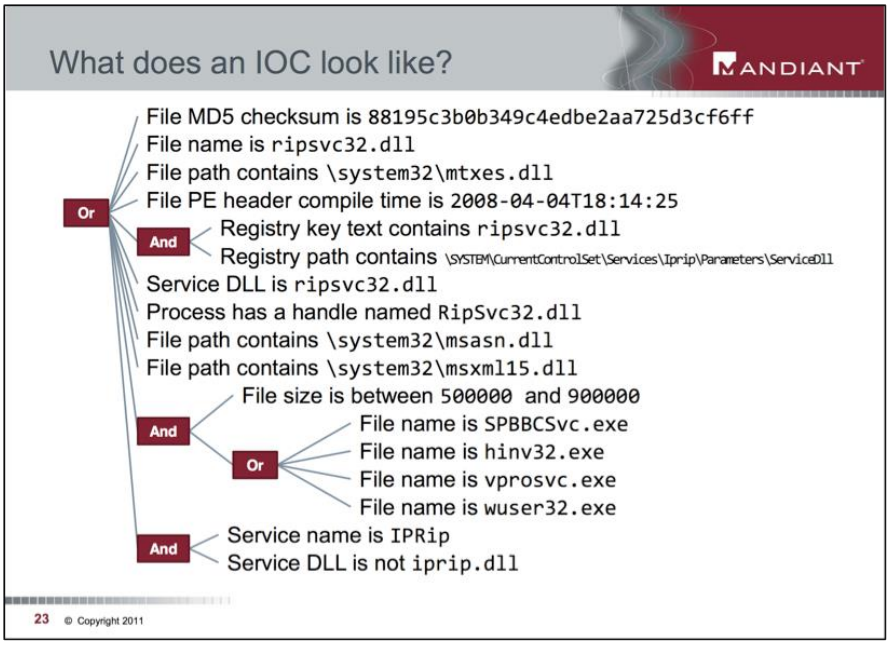


Figure 5: Indicators of compromise (Dittrich and Carpenter, 2016)

Table 2: Kill-chain, courses of action matrix and indicators (Hutchins et al., 2010)

Kill-Chain Phases	Activity	Indicators	Courses of Action (COA)					
			Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Destroy*
Reconnaissance	Research, Identification, and selection of targets	[Recipient List] Benign File: tcnom.pdf	Web Analytics	Firewall ACL				
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files	Trivial encryption algorithm: Key 1	NIDS	NIPS				
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drivers)	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Vigilant User	Proxy Filter	In-line AV	Queuing		
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems.	CVE-2009-0658 [shellcode]	HIDS	Patch	Data Execu-tion Pr-evention (DEP)			
Installation	The weapon installs a backdoor on a target's system allowing persistent access.	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp	HIDS	"chroot" jail	AV			
C2	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network	202.abc.xyz.7 [HTTP request]	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.	N/A	Audit Log			Quality of service	Honeypot	

The basic IOCs as detailed by Bianco (2014) in what he called his "Pyramid of Pain" (see Figure 6) are Hash Values, IP addresses, Domain names, Network/Host Artifacts, tools and TTPs (tactic, technique, procedure). This pyramid also shows the level of pain given to the adversary, should they pivot and continue with the planned attack, when the indicators at each of these levels are denied.

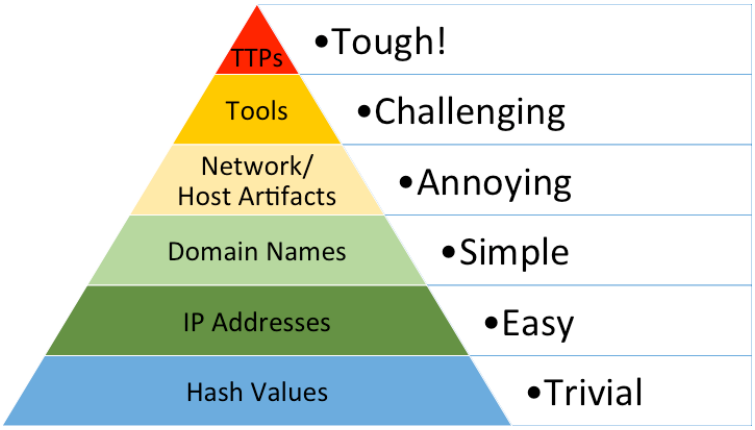


Figure 6: Pyramid of pain with IOCs (Bianco, 2014)

At the base of the pyramid is **Hash Values** (e.g. SHA1, MD5 or other similar hashes) often used to uniquely identify specific malware samples or malicious files found/involved in an attack. Even though hashes can be considered as the most accurate type of indicator, the adversary can easily change the hash value by altering an insignificant bit in the file and move forward. Moving to Fuzzy hashes can be a solution to this problem.

IP Addresses (e.g. IPv4 98.139.180.149 or IPv6 2002:4559:1FE2::4559:1FE2) are the most fundamental connection indicator. IP address denial is easy and quick to evade for an adversary using proxy service.

Domain Names (e.g. "evil.net" or "this.is.sooooo.evil.net") are mapping between an IP address and a URL. DNS request predicts the domain name connection requests made by any host. Domain name IOCs are useful to either monitor them for active connections or add to a blocklist for the future (Mack, 2015). The time to live (TTL) of an IP address in terms of IOC usage in a security deployment could be very low compared to the domain name. Changing domain names to evade detection involves registering

new name, paying for it maybe with fraudulent fund and hosting somewhere to make it visible to the internet which causes time delay for the adversary. Harder than evading IP addresses but is still doable.

Network Artifacts (URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values) and **Host Artifacts** (registry keys or values, files, directories, locations, names, services or anything that is distinctive) when detected and denied can have negative impact on the adversary causing them to expend effort in identifying giveaway artifacts, fixing, reconfiguring and recompiling their tools. The fix could be easy for the adversary but the long time to recover is annoying for them.

Tools (software, scripts) for IOC include utilities designed by the adversaries to maybe create malicious documents for spear-phishing, scripts opening backdoors utilized to establish C2 communication, or password crackers and maybe some other host-based utilities they want to use after a successful intrusion. AV or YARA signatures, network aware tools with a distinctive communication protocol, and fuzzy hashes can be used as IOC Tool indicators. Once the artifacts of the adversaries' tool(s) are detected, it is as if taking their weapons away from them. Now the adversaries must find or create a new tool - minus the detected artifacts - for the same purpose, get armed and train if needed, which will cost them considerable time.

When we detect and respond to **TTPs** (kill-chain phase actions that an adversary takes to accomplishing their mission)**,** we are operating at the level of adversaries' behavior and tendencies. Denying adversaries at this level, will force them to either learn new behaviors or reinvent themselves or just give up. TTPs are the ideal and most

valuable IOCs in terms of cyber defense. Spear-phishing with a trojaned PDF file or with a link to a malicious .SCR file disguised as a ZIP, dumping cached authentication credentials, and reusing them in Pass-the-Hash attacks are examples of TTPs.

There are many ways of representing indicators. YARA signatures are usually used for detecting malicious executables, and Snort/Bro can be used for detecting known signatures in network communications. Success of an attack investigation also depends on how confidently IOC evidences can be linked together with other events to understand adversaries' pattern of behavior. YARA can create free form signatures to tie indicators to actors and allow security analysts to look deeper than just hashes, IP addresses, and domains. This brings context to the investigation. Attack footprints are good, but we also must keep in mind that the footprints may change between attacks. IOCs offer hope, Patterns provide confidence.

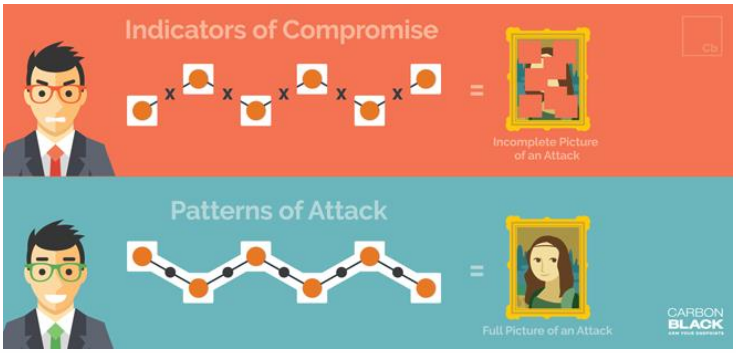


Figure 7: IOCs vs Patterning (Johnson, 2016)

Johnson (2016) explained the difference between Indicators and Patterns (Figure 7) with a simple burglary example that outlines the pattern as "When someone drives near the store late at night *THEN* attempts to enter the building *THEN* attempts to

deactivate the alarm *THEN* opens the register drawer, we almost *CERTAINLY* have an attempted burglary on our hands." and indicators as people with "blue shirt and short", "light hair color", "hiking backpack", "crowbar" etc.

A more relevant example of patterning was also given by Johnson (2016) as, "Outlook spawns Acrobat as a child to handle an attachment. That Acrobat then spawns an unsigned binary in a temporary user directory, which in turn spawns svchost.exe. That svchost is running as a non-typical user for that process."

Rudman and Irwin (2017) presented a detailed framework in their paper which shows automatic generation of IOCs from malware analysis. Their flowchart (see Figure 8) utilizes Cuckoo sandbox (an automated malware analysis system) to analyze malware sample that generates a PCAP file to record the network traffic information. Then this PCAP file gets trimmed using a custom processing module (tshark). From the filtered PCAP file, required properties were extracted using another custom reporting module to use for object data modeling. Lastly, python-cybox and python-stix libraries were utilized to generate actionable IOCs which was packaged before transportation to other CTI tools for scanning, monitoring and dissemination.

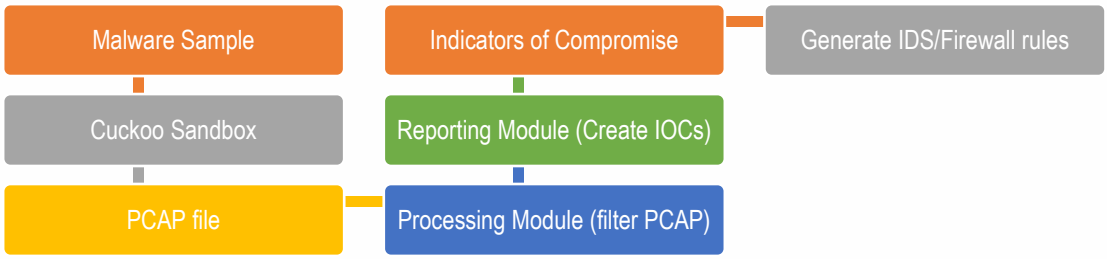


Figure 8: IOC analysis and creation flow diagram (Rudman and Irwin 2017)

IOCs represent threat intelligence in the cyber world. “Threat Intelligence framework is capable to provide enhanced evidence collection, actionable intelligence and central investigation for organization wide security solutions and open source intelligence feeds.” (Gheorghică and Croitoru, 2016). A new framework for enhanced measurable cybersecurity in computer networks was introduced in their paper (see Figure 9 below). Their modular design shows capabilities to provide enhanced evidence collection (data load and normalization), create actionable intelligence (advanced analytics) and central investigation portal (reporting and threat intelligence dissemination) for organization wide security solutions.

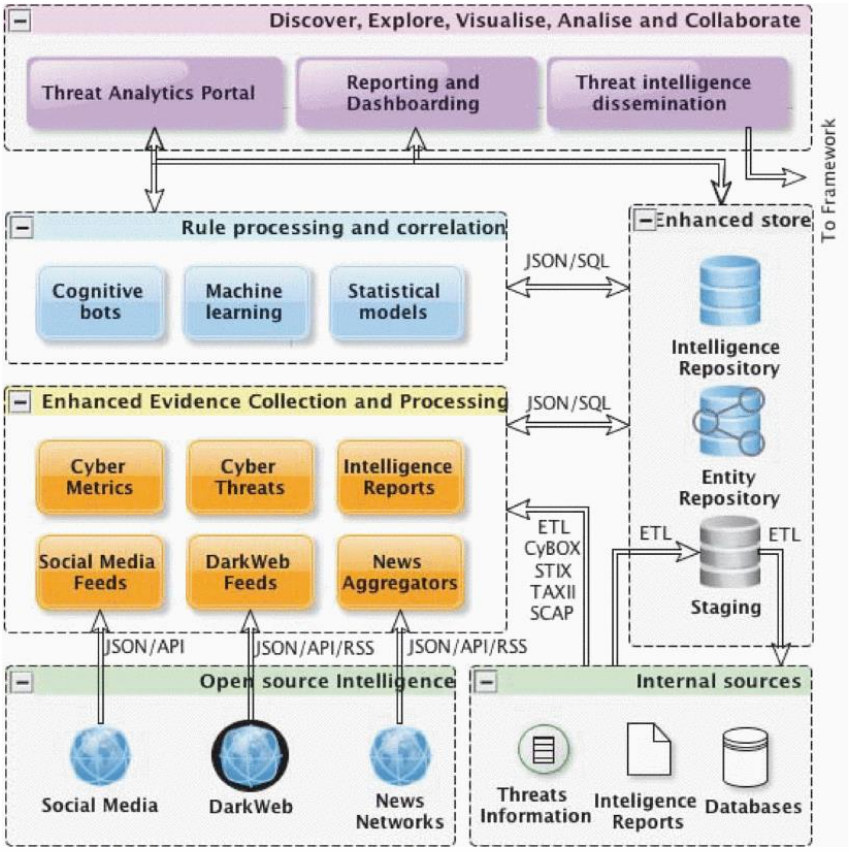


Figure 9: A new framework for TI (Gheorghică and Croitoru, 2016)

Summary

One of the major challenges organizations face while defending their network is being able to see enough of the network to identify recent most advanced, multi-vector threats. Ideally, organizations need to be able to see across the distributed network, including cloud deployments and devices from multiple network and security vendors. You then need to correlate detected local activity with global threat intelligence and expected behaviors and coordinate a response across the entire portfolio of installed security solutions.

Chapter III: Methodology

Introduction

The aim of this study is to provide a comprehensive overview that will help to understand the current CTI ecosystem and explore into STIX and TAXII frameworks as common standards. To be able to do that, information and references were collected in a methodical, trackable, and repeatable manner for them to be acceptable.

Design of the Study

The framework of the study was divided into three parts,

1. Tactics: Includes qualitative research on what is CTI, it's value to the organizations and why they are using CTI, how CTI can be leveraged to be proactively defend networks on the left side of the kill-chain, and government initiatives to encourage CTI sharing etc.
2. Techniques: Includes research on who are contributing to CTI development, how CTI can be used strategically as well as tactically to augment security efforts in organizations, where to source CTI from, standards facilitating structured sharing of CTI data amongst participating members, existing tools that generate, manage, and support different types of CTI data, and identifying the basic artifacts that may indicate an attack or compromise in a network.
3. Procedures: Includes research focusing on STIX 2.0 and TAXII 2.0 as the common standard under development for CTI sharing, exploring into the STIX

Core Concepts and Objects, STIX Observables Core Concepts and Objects, STIX Patterning, and also study the TAXII RESTful API framework.

Information Collection

Information for this study was collected using multistage sampling.

In the first stage, cluster sampling was used to group information requirements for each part of the study design. So, Tactics, Techniques and Procedures were each considered as a group based on information requirement.

In the second stage, purposive sampling was used to subjectively look for information relevant to each cluster or groups of information from the first stage. For example, to define CTI, a search with the string “What is CTI” can be used to source reference materials online.

At the last stage, random links from the search results of second stage were selected to look for acceptable publications or articles specific to the query (e.g. defining CTI) or purpose.

Information Analysis

To have a balanced understanding of the topic, a broad spectrum of information sources was considered. For this study, reference materials were analyzed from sources such as,

- GIAC (GCIH) Gold Certified research papers from SANS
- Peer-reviewed articles and journals
- Conference papers and presentations
- Government publications (gadgets, bulletins)

- Publications from Research organizations
- CTI survey reports
- Publications from service providers
- Framework specification documents
- Discussion forums
- News articles
- Blogs & Posts
- Websites
- Social Network posts

Summary

This chapter detailed the design of the study, multistage sampling in information collection and different sources for information analysis in the study. The methodical way of collecting information would be useful for anyone thinking about doing similar research work.

Chapter IV: Data Presentation and Analysis

Introduction

Collection of actionable Cyber Threat Intelligence (CTI) has been one of the top interests within the information security realm over the past few years. Given the increasing sophistications of adversaries, it has now become a necessity for the organizations to utilize the full potential of CTI through automation and readily process IOCs to analyze, detect and defend their network assets. Though the number of organizations taking part in development and implementation of CTI-enabled expert systems in their Security Operation Center (SOC) are increasing by the day, many still do not know how to take full advantage of CTI and fewer still are actually doing so. A SANS survey on “Who's Using Cyberthreat Intelligence and How?” by Shackleford (2015, p19), reveals that only 38% of respondents are using CTI data either utilizing a standard format or a well-known open source toolkit where,

- Open Threat Exchange (OTX) - 51%
- Structured Threat Information Expression (STIX) - 46%
- Collective Intelligence Framework (CIF) - 39%
- Open Indicators of Compromise (OpenIOC) framework - 33%
- Trusted Automated eXchange of Indicator Information (TAXII) - 33%
- Traffic Light Protocol (TLP) - 28%
- Cyber Observable eXpression (CybOX) - 26%
- Incident Object Description and Exchange Format (IODEF) - 23%
- Vocabulary for Event Recording and Incident Sharing (VERIS) - 20%

It is clear from above that even if OTX is a very popular tool, majority of the respondents are using the STIX and TAXII standards (CybOX now merged in STIX 2.0) most commonly in enterprise organizations as seen by Shackleford (2015). Even though STIX and TAXII standards are still under development, STIX became the most popular standard in 2017 with 40% closely followed by OpenIOC at 38% (Shackleford, 2017). However, in his recent survey report, Shackleford (2018) revealed that, “Most security teams are integrating CTI feeds into the environment using dedicated threat intelligence platforms (57%), followed by APIs (vendor-provided at 48%, followed closely by custom APIs at 46%)”. This is very promising for STIX and TAXII as a package.

Sharing of CTI through a common standard is the only way organizations can get ahead in this cyber battle against adversaries. In this chapter we will focus on the STIX 2.0 and TAXII 2.0 as the common standards to understand how CTI data are presented in JASON while converting sample IOCs to STIX format as examples and analyze the data flow of the TAXII 2.0 server and client.

Data Presentation in STIX 2.0 Standard

A brief introduction for OASIS CTI Technical Committee (TC), STIX and TAXII was covered in chapter-II of this paper. In short, Structured Threat Information eXpression (STIX) is an open source and free language and serialization format to efficiently characterize and communicate cyber threat intelligence. Trusted Automated Exchange of Indicator Information (TAXII) is the HTTPS/TLS protocol to transport and share STIX bundle.

STIX 1.x vs STIX 2.x. Powered by a collective community driven development, early users of STIX quickly noted the limitations of the STIX 1.x design choices in terms of the usefulness of the standard. STIX 2.0 was approved in March 2017 by OASIS CTI TC (2017) and built on the working foundation of STIX 1.2 reflecting with the community feedbacks. Figure 10 shows the objects defined in STIX 1.2 and STIX 2.0 architectures,

Figure 10: Comparison of STIX 1.2 and STIX 2.0 objects (MacDonald, 2017)

STIX 2.0 focused on developing a set of flexible building blocks for the content creators to easily model actual practice of threat intelligence. Key improvements in STIX 2.0 over STIX 1.2 includes (Wunder, 2017),

- STIX 1.x used XML as an exchange format, STIX 2.0 uses JSON. This matches common practice in development today and should drive adoption.
- STIX 1.x focused on flexibility, STIX 2.0 stresses simplicity and standardization. There are now fewer options and more requirements making STIX 2.0 easier to implement, a requirement for broad industry adoption.
- STIX 1.x contained connections, but by making it explicit, STIX 2.0 allows analysts and defenders to easily draw connections between seemingly unrelated data, follow chains from IOCs to the adversaries behind the compromise, and build out connections over time.
- CybOX (Cyber Observable Expression) has been merged into the STIX 2.0 specification. Now, STIX 2.0 is a multi-part specification with parts for STIX Core, STIX Objects, Cyber Observable Core, Cyber Observable Objects, and STIX Patterning.

STIX objects. STIX 2.0 is a graph-based model, where STIX Domain Objects (SDO), representing concepts in the cyber domain and used to describe things, are related to each other using STIX Relationship Objects (SRO). Complex representations of CTI can be expressed by connecting multiple SDOs through SROs. STIX 2.0 also uses ID references to represent embedded relationships (STIX-v2.0-Pt1-Core). A detailed introduction and visual representations for each STIX 2.0 SDOs and SROs can

be found at https://oasis-open.github.io/cti-documentation/stix/intro (For quick reference, see appendix A). However, for a quick understanding of the STIX 2.0 standard, let us cover some brief information collected from OASIS Committee Specification documents found at https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications.

As shown in Figure 10 above, STIX 2.0 specification (STIX-v2.0-Pt2-Objects) defines twelve SDOs (Attack Pattern, Campaign, Course of Action, Identity, Indicator, Intrusion Set, Malware, Observed Data (Observable), Report, Threat Actor, Tool, and Vulnerability) and two SROs (Relationship, Sighting). Figure 11 below shows an example of how STIX 2.0 SDO relationships are represented in graph and we note that the SDOs represent the ‘nodes’ while SROs represent the ‘edges’ of the graph.

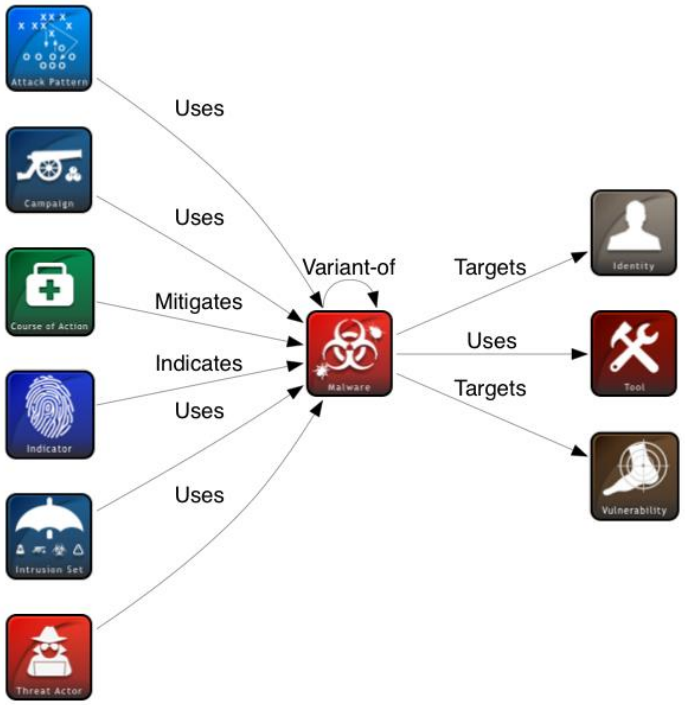


Figure 11: STIX 2.0 SDO relationship example (OASIS CTI TC, 2017)

Each STIX 2.0 SDOs and SROs have their own set of ‘properties’ that represent information specific to that object and ‘relationships’ that describes the way that object can be related to any other object. Some properties are common for all objects, some properties are required while others are optional for a particular object. JSON (JavaScript Object Notation), which is a data-interchange format, is used to express STIX 2.0 information as serialized objects. More on JSON can be found at http://www.json.org/. An example of STIX 2.0 Indicator Object representation in JSON is given below where type, id, created_by_ref, created, modified and labels are common properties and type, labels, pattern and valid_from are required properties for the Indicator Object.


```
{
   "type": "indicator",
   "id": "indicator--8e2e2d2b-44d4-4cbf-938f-34ee46b3cd3f",
   "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
   "created": "2018-03-03T20:03:48.000Z",
   "modified": "2018-03-03T20:03:48.000Z",
   "labels": ["malicious-activity"],
   "name": "Poison Ivy Malware",
   "description": "This file is part of Poison Ivy",
   "pattern": "[ file:hashes.'SHA-256' =
'4bac27393bdd9333ce02453256c5533cd02275510b2227f473d03f533924f877' ]",
   "valid_from": "2018-01-01T00:00:00Z"
 }
```


According to the STIX 2.0 specification, the id property universally and uniquely identifies an SDO, SRO, Bundle, or Marking Definition. It must follow the format ‘object-type--UUIDv4’, where object-type is the exact value from the type property of the object being identified or referenced and UUIDv4 is RFC 4122-compliant. Timestamps are in UTC time zone (indicated by “Z”) and follow the format YYYY-MM-DDTHH:mm:ss.000Z.

Also, all type names (separated by ‘-‘), property names (separated by ‘_’), and literals (separated by ‘-’) should be in lowercase and between 3-250 characters.

Apart from the STIX 2.0 Relationship object, the only other type of SRO currently defined in STIX 2.0 is the Sighting Object which allows CTI sharing communities to provide feedback when a STIX 2.0 object is seen in their network. It requires sighting_of_ref property to reference the sighted object.

Marking definition contains the actual data markings applied to STIX objects by using the object_marking_refs and granular_markings properties. While being open to all sorts of data markings, STIX 2.0 specification (STIX-v2.0-Pt1-Core) defines ‘TLP’ to capture the Traffic Light Protocol markings and ‘Statement’ to capture text marking i.e. terms of use. Marking definitions cannot be versioned like other STIX 2.0 Objects to prohibit indirect changes to the same markings used in different STIX 2.0 objects.

A Bundle is a container object that is used to group together a collection of STIX 2.0 Objects for transportation and sharing. A Bundle does not have any semantic meaning and Objects in the same bundle may or may not be related to each other. A Bundle does not have any common properties except the required type, id and spec_version (indicating STIX specification) properties as it is not a STIX 2.0 object. The list of collected STIX 2.0 Objects are then contained in the objects property list. Bundle is transient, and STIX 2.0 implementations should not assume it as a persistent object. An example follows (STIX-v2.0-Pt1-Core),


```
{
  "type": "bundle",
  "id": "bundle--8e2e2d2b-44d4-4cbf-938f-34ee46b3cd3f ",
  "spec_version": "2.0",
```

```
"objects": [
  {
    "type": "indicator",
    …
  },
  {
    "type": "malware",
    …
  },
  {
    "type": "relationship",
    …
  } ] }
```

'STIX 2.0 Producer' is the entity that creates an Object and 'STIX 2.0 Consumer' is the entity that receives an object created using STIX 2.0 SDOs and SROs.

Cyber observables objects. The common data types used throughout STIX 2.0 are Boolean, external-reference, float, hashes, identifier, integer, kill-chain-phase, list, open-vocab, string and timestamp. STIX 2.0 also uses binary, hex, dictionary, object-ref and observable-objects as additional data types specifically for Cyber Observable Object types (STIX-v2.0-Pt3-Cyb-Core). These observable objects are required in STIX 2.0 to describe structured representation of SDO and SRO properties in the cyber domain with greater details. These objects can describe one or more observed data points or IOCs to characterize host-based, network, and related entities.

STIX 2.0 specification (STIX-v2.0-Pt4-Cyb-Objects) defines eighteen Observable object data models - Artifact Object, AS Object, Directory Object, Domain Name Object, Email Address Object, Email Message Object, File Object, IPv4 Address Object, IPv6 Address Object, MAC Address Object, Mutex Object, Network Traffic Object, Process Object, Software Object, URL Object, User Account Object, Windows™ Registry Key

Object, and X.509 Certificate Object. Relationships in Cyber Observable Objects are references represented as properties of an Observable Object containing the keys of the target Cyber Observable Object(s) within the scope of the dictionary. However, to encode additional data beyond the defined Object data models, STIX 2.0 permits additional properties through Predefined Cyber Observable Object Extensions. Following example shows an ICMP Network Traffic with Source / Destination IPv4 Addresses, extensions properties and AS (autonomous-system) using Object Models. The belongs_to_refs property in the first IPv4 Address Object specifies that the only valid target of the relationship is one or more AS Object(s).

```
{
 "0": {
  "type": "ipv4-addr",
  "value": "198.35.100.2",
  "belongs_to_refs": ["3"]
 },
 "1": {
  "type": "ipv4-addr",
  "value": "198.35.100.3"
 },
 "2": {
  "type": "network-traffic",
  "src_ref": "0",
  "dst_ref": "1",
  "protocols": [
   "icmp"
  ],
  "extensions": {
   "icmp-ext": {
    "icmp_type_hex": "08",
    "icmp_code_hex": "00"
   }
  } };
 "3": {
  "type": "as"
  "number": 42, …
 } }
```

STIX patterning. According to STIX 2.0 specification (STIX-v2.0-Pt5-Patterning), “STIX Patterning language allows matching against timestamped Cyber Observable data collected by a threat intelligence platform or similar system so that other analytical tools and systems can be configured to react and handle incidents that might arise.” Unlike others, STIX Patterning is a cross domain, SQL like language for describing chaotic maliciousness one might see. A rule for what to search for using temporal operators and modifiers. A simple example of STIX Patterning is shown in Figure 12 where an Observation Operator is used to specify that an observation of a domain name ‘z’ must follow the observation of the IP addresses ‘x’ or ‘y’, along with a different Qualifier to state an observation window ‘600 Seconds’.

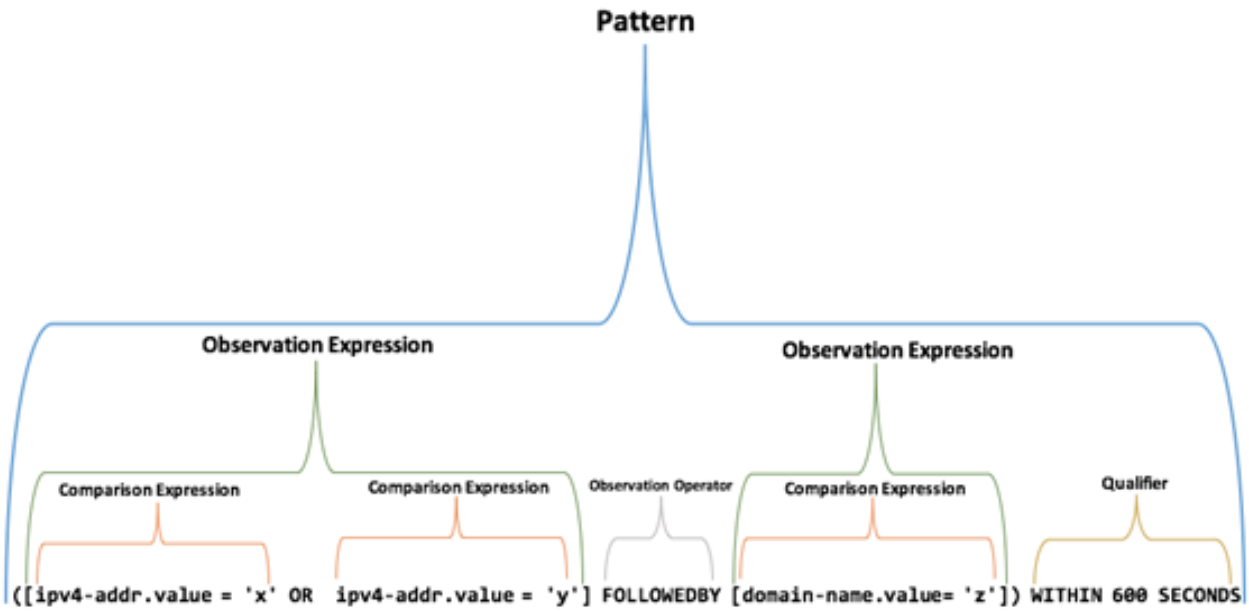


Figure 12: STIX 2.0 Patterning (STIX-v2.0-Pt5-Patterning)

Following two examples illustrates STIX Indicator Patterns equivalent to YARA and SNORT rules (Darley and Keirstead, 2017),

STIX Indicator Pattern for Basic File with Hexadecimal Payload

```
[file:contents_ref.payload_bin
MATCHES '\\x43\\x78\\x77\\x6c\\x70\\x6a\\x68'
AND file:size > '32152']
```

Corresponding YARA Rule,

```
rule Example
{
        strings: $hex_string = { 43 78 77 6c 70 6a 68 }
        condition: $hex_string and filesize > 32152
}
```

Again, STIX Indicator Pattern for basic TCP Network Traffic,

```
[network-traffic:src_ref.type = 'ipv4-addr'
AND network-traffic:src_ref.value = '192.35.100.5'
AND network-traffic:dst_ref.type = 'ipv4-addr'
AND network-traffic:dst_ref.value = '203.66.200.6'
AND network-traffic:dst_port = '21'
AND network-traffic:protocols[*] = 'tcp']
```

Corresponding SNORT Rule,

```
alert tcp 192.35.100.5 any -> 203.66.200.6 21
```

Now that we understand how CTI data is represented in STIX 2.0 Standard, we can try to convert some IOCs to STIX format before exploring into TAXII 2.0 Standard.

Converting IOCs to STIX 2.0 Standard

IOCs, explained earlier in Chapter II as Pyramid of Pain (Bianco, 2014), are expressed using Cyber Observable Objects in STIX 2.0 standard and are used by various STIX Domain Objects (SDO), specially the Observed Data SDO. Including multiple Cyber Observable Objects in a single SDO instance is possible when they are

related. However, it is best practice to use separate SDOs for unrelated data. Earlier example (ICMP network traffic) in this chapter shows representation of IP Address and Network Artifact. We are going to see some more IOC representations in STIX 2.0 standard in this section.

Following example shows a STIX 2.0 bundle with three unrelated observed data SDOs and a Tool SDO. For each observed-data object, first_observed, last_observed and number_observed properties are required apart from the common properties. Also, the cyber observable objects (IOCs) needs to be included in the SDO's property. As we can see here, the first Observed-data SDO contains the file hashes, name, and size to represent the file and it was seen only once by the STIX producer as in created_by_ref property. The second Observed-data SDO is created by the same producer and contains a Windows Registry key value that may have been created by a malware and was observed once. The third Observed-data SDO contains a basic HTTP network traffic for an interesting domain name 'g00gle.com' that resolves to an IPv4 address of '198.11.100.44'. This was observed 47 times by the same producer. The fourth object in the bundle created by the producer is a Tool SDO that contains a remote access software 'VNC' which may have been used by threat actor(s) to perform attacks. Some common object properties are truncated for brevity.


```
{
  "type": "bundle",
  "id": "bundle--a836f05a-f235-4b4b-b523-bd87e40478a1",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "observed-data",
      "id": "observed-data--cf8eaa41-6f4c-482e-89b9-9cd2d6a83cb1",
```

```
  "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
  "created": "2017-02-28T19:37:11.213Z",
  "modified": "2017-02-28T19:37:11.213Z",
  "first_observed": "2017-02-27T21:37:11.213Z",
  "last_observed": "2017-02-27T21:37:11.213Z",
  "number_observed": 1,
  "objects": {
    "0": {
      "type": "file",
      "hashes": {
            "MD5": "1717b7fff97d37a1e1a0029d83492de1",
            "SHA-1": "c79a326f8411e9488bdc3779753e1e3489aaedea"
      },
      "name": "creamcheese.pdf",
      "size": 55896
    }
  } },
{
  "type": "observed-data",
  "id": "observed-data--a0d34360-66ad-4977-b255-d9e1080421c4",
  "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
  ……
  "number_observed": 1,
  "objects": {
    "0": {
      "type": "windows-registry-key",
      "key": "HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Services\\WSALG2"
    }
  } },
{
  "type": "observed-data",
  "id": "observed-data--9518e286-2b38-11e8-b467-0ed5f89f718b",
  "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
  ……
  "number_observed": 47,
  "objects": {
    "0": {
      "type": "domain-name",
      "value": "g00gle.com",
      "resolves_to_refs": [
        "2"
      ]
    },
    "1": {
      "type": "network-traffic",
```

```
        "dst_ref": "0",
        "protocols": [
          "ipv4",
          "tcp",
          "http"
        ]
      },
      "2": {
        "type": "ipv4-addr",
        "value": "198.11.100.44"
      }
    } },
{
  "type": "tool",
  "id": "tool--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created_by_ref": "identity--987eeee1-413a-44ac-96cc-0a8acdcc2f2c",
  ……
  "labels": [ "remote-access"],
  "name": "VNC"
} ] }
```


IOCs are very time sensitive and useful when shared and acted upon quickly. This is where automation is crucial and TAXII can help transport STIX content freely and securely across networks.

Data Communication through TAXII 2.0 Standard

TAXII as mentioned in Chapter II of this document, is an application layer protocol used for CTI data transportation over HTTPS/TLS. It works as a protected repository for IOC collection and sharing as well as compare information. It also allows to record and share suspicious traffic log activities translated into universal format. Though TAXII 2.0 supports other data standards, it is specifically optimized to exchange CTI represented in STIX and support for STIX 2.0 content is mandatory to implement. The complete TAXII Committee Specification document referenced for this section can be found at http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-

cs01.html#_q0a03pfr5x7n. The following section covers higher-level understanding of data flow in TAXII 2.0 standard.

Figure 13 shows the different components and services in a TAXII 2.0 structure. TAXII defines a RESTful API (or web service) with two primary services, Collections and Channels, to support various sharing models (i.e.peer-to-peer, source-subscriber, hub-and-spoke). TAXII Servers uses DNS service record to advertise its network location internally or externally and must use the service name ‘taxii’. **Discovery** methods (Network and Endpoint) are used to get the location, supported services and capabilities of the TAXII Server and its API Root(s).

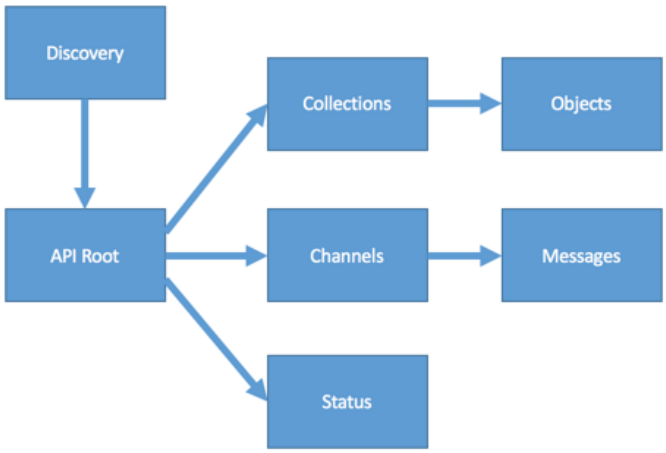


Figure 13: API root components (TAXII-v2.0)

An instance of TAXII server API supports multiple **API Roots** to facilitate logical grouping of services needed by a CTI sharing community, trust groups, organizations etc. In this case, each API Root will be considered as the ‘root’ URL for that group and will have their own defined endpoints for information collection using Discovery.

Collections provided by the TAXII Server API Root(s) is a repository for CTI **objects** (sorted using added date in ascending) that exchanges information with a TAXII Client in request-response manner. **Channels** on the other hand is a way for authorized TAXII Clients to communicate **messages** with other authorized TAXII Clients in the same TAXI Server channel using publish-subscribe model. See Appendix B and C for better visuals on TAXII 2.0 deployments and channel communication. Each API Root can host multiple Collections and Channels. In TAXII 2.0, **Status** request allows a TAXII Client to check on CTI object submission requests for Collections with the TAXII Server. Figure 14 shows the concepts of Collections and Channels with their data flows,

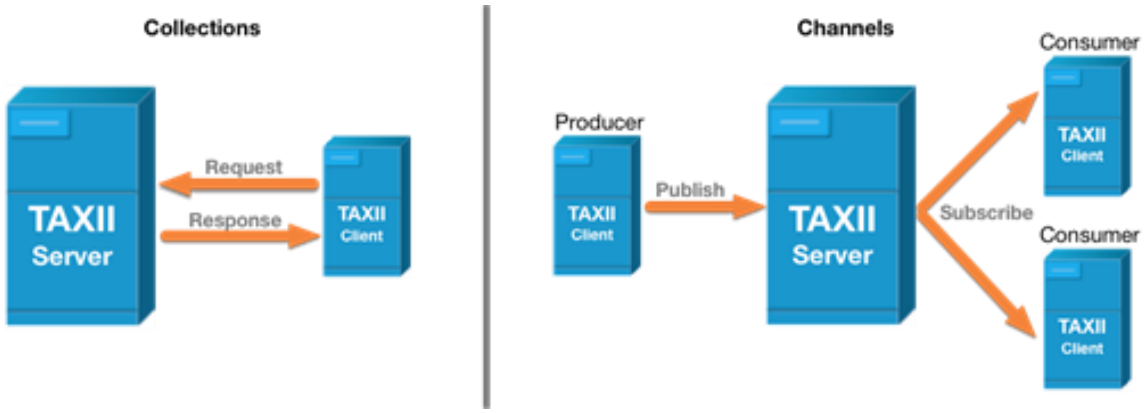


Figure 14: Channels and Collections communicaton (TAXII-v2.0)

TAXII 2.0 standard (TAXII-v2.0) uses the following to define data types - api-root, Boolean, bundle, collection, collections, dictionary, discovery, error, identifier, integer, list, manifest, object, status, string and timestamp.

TAXII 2.0 uses HTTP for authentication and content negotiation only. TAXII Clients must include an acceptable authorized header, granting their access to an

object, while requesting through Endpoints that require authentication or the TAXII Server rejects the request with a HTTP 401 code ‘Unauthorized’ and WWW-Authenticate header.

Summary

Data integration has always been a challenge for data providers or data integrators due to the differences in proprietary data formats. Limitations also exist in capabilities of devices and software used in network security and monitoring. STIX 2.0 offers a common language for data presentation utilizing JSON that all vendors can easily follow through and eventually get rid of the interoperability issues between sharing systems. In this chapter we have studied all five STIX 2.0 specification documents published thus far to understand and summarize how data is represented through SDOs, SROs, Versioning, Data Marking, Patterning and Cyber Observable Objects. We explored the improvements of STIX 2.0 over STIX 1.2 and looked at some examples of how IOCs are expressed in SDOs using Cyber Observable Objects. We have also studied TAXII specification document to understand the components in a TAXII 2.0 API and data flow in a TAXII 2.0 Server-Client model through Collections and Channels. Now, it is time to plug in all the information we have studied so far in this paper and draw some conclusions in the next chapter.

Chapter V: Results, Conclusion, and Recommendations

Introduction

The objective of this paper was to learn about the different parts of Cyber Threat Intelligence (CTI) ecosystem and how this complex structure can be expressed through STIX 2.0 and TAXII 2.0 standards for proactive cyber defense. In this chapter, we will summarize what we have learned thus far and draw some concluding remarks. We will also look at some future work that can be done with support of the knowledge learned from this paper.

Results

This study of the current CTI landscape reveals that, “Threat intelligence is currently very loosely defined, with little agreed consensus on what it is and how to use it. There is a risk that in the hurry to keep up with the threat intelligence trend, organizations will end up paying large amounts of money for products that are interesting but of little value in terms of improving the security of their business. ‘Doing’ threat intelligence is important – but doing it right is critical.” (Chismon and Ruks, 2015). We understand that CTI should be utilized to collect actionable information on the adversary’s capabilities, intentions, and ongoing activity useful to the enterprise defense. Shortening the window between a compromise and when that compromise is detected is the key and possible only by fast and reliable CTI sharing. The goal of such effort leads to risk mitigation by profiling and predicting attacks to block on the left side of the kill-chain. The challenge however, lies in collecting quality and actionable IOCs that can be minimized by having better interoperability across security tools through

establishing common standards. Having common standards also allow CTI vendors to integrate off the shelf that saves money for both vendor and the client.

Valuable CTI is available in both industry and government. Regulatory compliance guidelines and laws are not enough to safeguard critical data. Collective defense approach is only possible when all parties increase their CTI sharing. Time critical nature of CTI demands quick action and seamless integration, but organizations are not always at liberty to share. Department of Homeland Security (DHS) handed over the development of global foundational cyber security specification (STIX, TAXII and CybOX) to OASIS Cyber Threat Intelligence Technical Committee (OASIS CTI TC) on May 2015 with a hope for better collaboration and broader acceptance across the globe as sometimes, it is regarded that sending information to the government is a one-sided communication. OASIS CTI TC (2017) recently published their Committee Specification 01 for STIX 2.0 and TAXII 2.0 standards in July 2017 with some major changes. Currently, they are working on STIX 2.0 and TAXII 2.0 interoperability specification document and building out tools to support backward compatibility, more conversions and better integration.

Approaches to CTI is based on the consumer and what they aim to achieve from it. Project Management Body of Knowledge (PMBOK) is an accepted standard and will be a good choice for complex CTI projects to increase the odds for success. The board however needs high-level information on changing risk and a strategic approach to CTI is more appropriate for them whereas a tactical approach is more relevant down the ladder. Figure 15 shows a typical CTI team in an organization and their data

requirement. Organization with several sister concerns or global presence in difference locations can benefit from trust group or focused group approach to CTI.

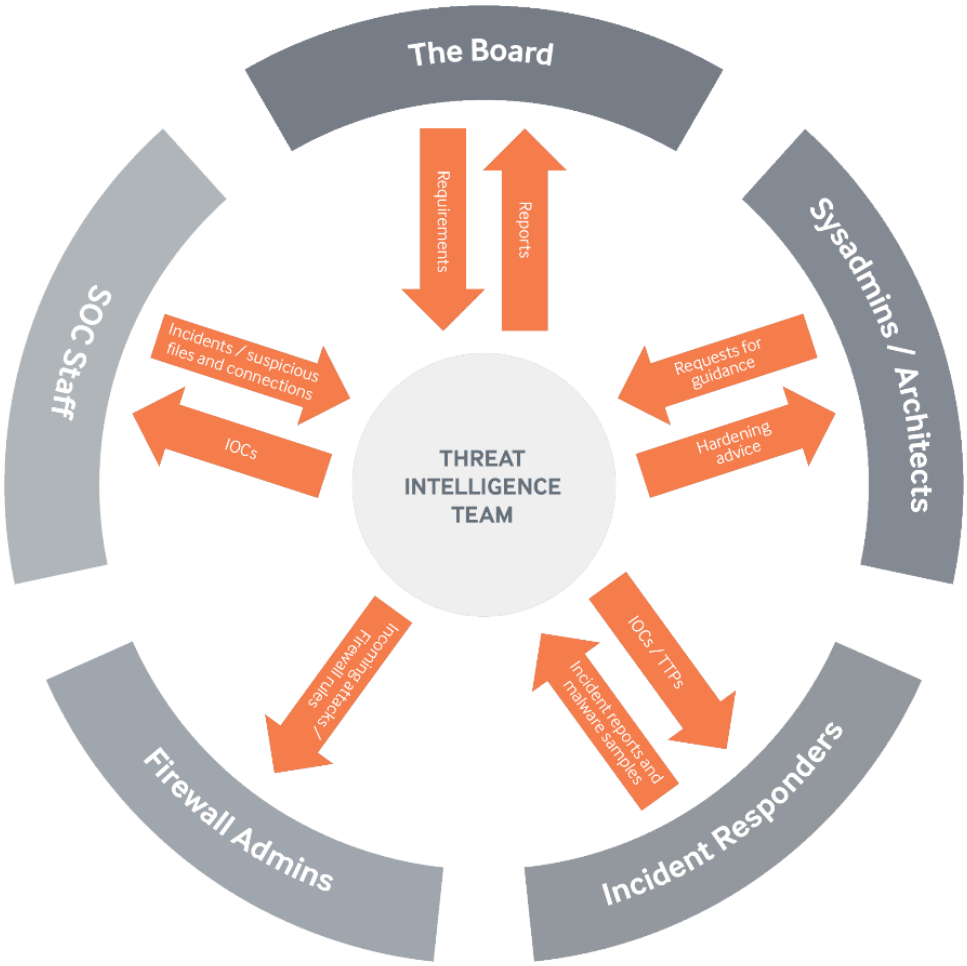


Figure 15: CTI team (Chismon and Ruks, 2015)

During our study, we have looked into different sources of CTI. Organizations should plan to incorporate as many credible sources (Internal, External, Community, HUMINT) as they can, keeping in mind their relevance to the threat defense infrastructure and if the collected CTI is actionable. We learned from studying the

existing CTI sharing standards that many standards will fit a specific organizational need i.e. Vocabulary for Event Recording and Incident Sharing (VERIS) to share incident data for analysis of a broad data set, Open Threat Exchange (OTX) to share indicator details in a public system, Open Indicators of Compromise (OpenIOC) to support their tools when used. The Managed Incident Lightweight Exchange (MILE) package (IODEF, IODEF-SCI, RID) and the MITRE package (STIX, TAXII) can be used to represent and transport data efficiently (Farnham, 2013). STIX 2.0 and TAXII 2.0 has been significantly improved over their predecessors. They are more efficient and can model things more accurately across CTI domains.

Data Feed Providers (DFP) i.e. STAXX, Recorded Future, Hali A TAXII, OTX, Limo etc. acts as producers of STIX 2.0 content and OSINT for threat library. Threat Intelligence Platforms (TIP) i.e. ThreatConnect, ThreatStream, Soltra, Arbor Networks, iSIGHT etc. acts as producer and/or respondent of STIX 2.0 content and are primarily used to aggregate, refine, and share CTI across security infrastructure with other devices or security personnel. Security Incident and Event Management systems (SIEM) i.e. ArcSight, Splunk, QRadar etc. also acts as producer (typically creates incidents and indicators) and/or respondent (typically consumes sightings and indicators) of STIX 2.0 content. Threat Mitigation System (TMS) i.e. Hexadite, IBM, LogRhythm Phantom Cyber, Rapid7 etc. acts on courses of action and other threat mitigations such as firewall or IPS, Endpoint Detection and Response (EDR) etc. Threat Detection System (TDS) i.e. Snort, Bro, web proxy etc. monitors, detects and alerts based on signature matching or anomalies in data flow. Threats are constantly evolving,

and the CTI tools used in a security infrastructure must constantly update to be at par with the trend. The effectiveness of defense is only as good as the ability of the network security devices that support it.

"Each specific IOC, be it shared via intelligence collaboration or collected internally, has a reason for its existence and a corresponding set of network technologies that would make the best choice for the implementation of detective and preventive controls." (Mack, 2015). More work needs to be done to accurately identify IOCs in a network traffic. Three things are important when it comes to IOCs, that they are accurate from the beginning, are actionable and they should be acted upon while they have a useful lifetime.

Conclusion

The rise of CTI is obvious when we see legacy firms revamped their CTI practices and offering, investors find new CTI startups interesting, tracking is hard for rapidly growing CTI data feeds (see http://threatintelligencereview.com/). It is beyond confusion at this moment that Cyber Threat Intelligence (CTI) is rapidly becoming a business priority and the need for sharing is now given. CTI providers and TIP vendors are starting to realize that their threat detection technique and information presentation may differ, but they must come to common terms with a standardized expression language to deal with interoperability issues. Offering confusingly diverse array of CTI products is just not helping anymore. Our study of STIX 2.0 and TAXII 2.0 standard revealed that the adoption of STIX and TAXII standards has rapidly increased in the past few years. World's largest crowd-sourced CTI provider and platform Alienvault's

Open Threat Exchange (OTX) has updated their capability to provide service as a STIX/TAXII server (Doman, 2017). ThreatConnect (2017), a TIP for analytics and automation, also integrated STIX and TAXII into their products. These actions tell us the story of a change-shift in process where STIX and TAXII is quickly taking control as a package for CTI sharing standard for all sharing parties whether they are industry, government or individual to react rapidly to new threats. “Knowing the threat will help you share intelligence on the threat and will help you craft the best intelligence sharing programs, so, never stop studying the threat” (Gourley, 2015).

Future Work

When it comes to supporting analyst tradecraft, there is still much to be done. Features being discussed for inclusion in upcoming versions of STIX 2.x include (MacDonald, 2017),

- Cryptographic authentication of threat intelligence to prove who produced it.
- The ability to agree or disagree with assertions from other intelligence producers, allowing an analyst to recognize bad threat intelligence.
- Ability to ask a question to the community and assess responses (e.g. “Does anyone have threat intelligence about 1.2.3.4?”).
- Improved description of confidence levels (e.g. Admiralty code).
- Addition of Incident Object.
- Addition of Infrastructure Object.
- Expanded number of CybOX objects to record more types of observed data.

In addition, according to their official github (https://github.com/oasis-tcs/cti-stix2) OASIS CTI TC is also planning to introduce in STIX 2.x features such as Enhanced malware capabilities, Location Object, and Internationalization Object along with many enhancements and bug fixes.

The information gained from this study is expected to form a basic understanding of how CTI landscape is laid out, available standards and tools, CTI sources, IOCs and most importantly an understanding of STIX 2.0 and TAXII 2.0 standard. This knowledge will be helpful for the reader in implementing first a TAXII Client (see useful link in Appendix D) as a next step and connect to a DFP such as OTX or Hail A TAXII to test with subscribed collections and channels. Then implement a TAXII 2.0 server and test its API functions. Both github repositories for TAXII client and server is very detailed and easy to follow. Implementing TAXII server and client in a publisher-subscriber model could be an exciting paper or thesis for anyone interested to learn how to automate CTI sharing through TAXII and STIX bundle. Implementing STIX and TAXII in an actual security operations environment could be challenging while the standards are still under development. But the rapid adoption of STIX and TAXII by the growing community shows promising future and the knowledge will last for a long time.

References

Athias, J. (2015), Cyber Threat Intelligence Sharing Standards, Retrieved 10/06/2017 from RSA Conference, https://www.rsaconference.com/writable/presentations/file_upload/pst-w08-cyber-threat-intelligence-sharing-standards.pdf

Badger, L., & Johnson, C., & Waltermire, D., & Snyder, J., & Skorupka, C. (2016), Guide to Cyber Threat Information Sharing, Retrieved 10/04/2017 from NIST, http://dx.doi.org/10.6028/NIST.SP.800-150

Bianco, D. (2014, Jan 17), The Pyramid of Pain, Retrieved 10/14/2017 from, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bromiley, M. (2016), Threat Intelligence: What It Is, and How to Use It Effectively, Retrieved 11/14/2017 from SANS, https://www.sans.org/reading-room/whitepapers/threathunting/threat-intelligence-is-effectively-37282

Chismon, D., & Ruks, M. (2015), Threat Intelligence: Collecting, Analysing, Evaluating, Retrieved 15/03/2018 from MWR, https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf

CSIRTGadgets, Collective Intelligence Framework, Retrieved 10/09/2017 from CSIRTGadgets, http://csirtgadgets.org/#canvas

CyberEdge (2017), 2017 Cyberthreat Defense Report, Retrieved 10/04/2017 from Cyber-Edge, https://cyber-edge.com/wp-content/uploads/2017/06/CyberEdge-2017-CDR-Report.pdf

Darley, T., & Keirstead, J. (2017, Dec 14), STIX Patterning: Viva la revolución!, Retrieved 02/03/2018 from FIRST, https://www.first.org/resources/papers/prague2017/Wednesday-Session-3.pdf

Dittrich, D., & Carpenter, K. (2016, Apr 21), Misunderstanding Indicators of Compromize, Retrieved 11/14/2017 from Threatpost, https://threatpost.com/misunderstanding-indicators-of-compromise/117560/

Doman, C. (2017, Apr 27), OTX Is Now a Free STIX/TAXII Server, Retrieved 15/03/2018 from Alienvault, https://www.alienvault.com/blogs/security-essentials/otx-is-now-a-free-stix-taxii-server

Farnham, G. (2013), Tools and Standards for Cyber Treat Intelligence Projects, Retrieved 10/04/2017 from SANS, https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

Gheorghică, D., & Croitoru, V. (2016), A new framework for enhanced measurable cybersecurity in computer networks, Retrieved 15/03/2018 from IEEE, http://ieeexplore.ieee.org.libproxy.stcloudstate.edu/stamp/stamp.jsp?tp=&arnumber=7528209&isnumber=7528195

Gourley, B. (2015, Sep 9), Cyber Threat Intelligence Sharing: Lessons Learned, ObservaMons, RecommendaMons, Retrieved 15/03/2018 from NIST, https://csrc.nist.gov/CSRC/media/Presentations/Cyber-Threat-Intelligence-Sharing-Lessons-Learned/images-media/day1_info-sharing_100-150.pdf

Hutchins, E. M., & Cloppert, M. J., & Amin, R. M. (2010), Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Retrieved 11/14/2017 from Lockheed Matrin, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Johnson, B. (2016, May 10), Patterns of Attack: You're Looking for Answers, Not Just Indicators, Retrieved 11/14/2017 from Carbon Black, https://www.carbonblack.com/2016/05/10/patterns-of-attack-youre-looking-for-answers-not-just-indicators/

Johnson, C., & Feldman, L., & Witte, G., & Editors (2017, May), Cyber-Threat Intelligence and Information Sharing, Retrieved 10/05/2017 from NIST ITL Bulletin, https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2017-05.pdf

MacDonald, T. of Cosive (2017), Whitepaper: STIX 2.0. Build your own intel, Retrieved 11/14/2017 from EclecticIQ, https://www.eclecticiq.com/resources/white-paper-stix-2-0-build-your-own-intelligence#download

Mack, J. (2015), Using Network Based Security Systems to Search for STIX and TAXII Based Indicators of Compromise, Retrieved 10/04/2017 from SANS, https://www.sans.org/reading-room/whitepapers/detection/network-based-security-systems-search-stix-taxii-based-indicators-compromise-36147

McMillan, R. (2013, May 16), Definition: Threat Intelligence, Retrieved 10/04/2017 from Gartner, https://www.gartner.com/doc/2487216?ref=SiteSearch&sthkw=G00249251

Metivier, B. (2016, Jul 12), A Guide to Cyber Threat Intelligence Sources, Retrieved 11/14/2017 from Sage Data Security, https://www.sagedatasecurity.com/blog/guide-to-cyber-threat-intelligence-sources

MITRE (2017), Threat Based Defense, Retrieved 10/14/2017 from https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

NICT-CYBEX Forum, Overview of IODEF-SCI, Retrieved 10/09/2017 from NICT, http://cybex.nict.go.jp/iodef-sci_en.html

OASIS CTI TC (2017), CTI-Documentation, Retrieved 11/02/2017 from OASIS-Open github, https://oasis-open.github.io/cti-documentation/

Poputa-Clean, P. (2015), Automated Defense - Using Threat Intelligence to Augment, Retrieved 10/04/2017 from SANS, https://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligence-augment-35692

Rudman, L., & Irwin, B. (2017), Dridex: Analysis of the traffic and automatic generation of IOCs, Retrieved 15/03/2018 from IEEE, http://ieeexplore.ieee.org.libproxy.stcloudstate.edu/stamp/stamp.jsp?tp=&arnumber=7802932&isnumber=7802913

Shackleford, D. (2015), Who's Using Cyberthreat Intelligence and How?, Retrieved 11/05/2017 from SANS, https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767

Shackleford, D. (2016), The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing, Retrieved 10/06/2017 from SANS, https://www.sans.org/reading-room/whitepapers/analyst/state-cyber-threat-intelligence-survey-cti-important-maturing-37177

Shackleford, D. (2017), Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey, Retrieved 03/04/2018 from SANS, https://www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677

Shackleford, D. (2018), CTI in Security Operations: SANS 2018 Cyber Threat Intelligence Survey, Retrieved 03/04/2018 from SANS, https://www.sans.org/reading-room/whitepapers/analyst/cti-security-operations-2018-cyber-threat-intelligence-survey-38285

St.Clair, A. (2017, Mar 6), Cyber Threat Intelligence -Tactical, Operational and Strategic layers, Retrieved 10/05/2017 from Linkedin, https://www.linkedin.com/pulse/cyber-threat-intelligence-tactical-operational-layers-st-clair

STIX-v2.0-Pt1-Core, STIX™ Version 2.0. Part 1: STIX Core Concepts. Edited by Rich Piazza, John Wunder, and Bret Jordan. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html.

STIX-v2.0-Pt2-Objects, STIX™ Version 2.0. Part 2: STIX Objects. Edited by Rich Piazza, John Wunder, and Bret Jordan. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.htmll. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html.

STIX-v2.0-Pt3-Cyb-Core, STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts. Edited by Trey Darley and Ivan Kirillov. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part3-cyber-observable-core/stix-v2.0-cs01-part3-cyber-observable-core.html. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part3-cyber-observable-core.html.

STIX-v2.0-Pt4-Cyb-Objects, STIX™ Version 2.0. Part 4: Cyber Observable Objects. Edited by Trey Darley and Ivan Kirillov. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part4-cyber-observable-objects/stix-v2.0-cs01-part4-cyber-observable-objects.html. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html.

STIX-v2.0-Pt5-Patterning, STIX™ Version 2.0. Part 5: STIX Patterning. Edited by Trey Darley and Ivan Kirillov. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part5-stix-patterning/stix-v2.0-cs01-part5-stix-patterning.html. Latest version: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html.

TAXII-v2.0, TAXII™ Version 2.0. Edited by John Wunder, Mark Davidson, and Bret Jordan. 19 July 2017. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html. Latest version: http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html.

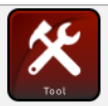
The VERIS Framework, VERIS - the vocabulary for event recording and incident sharing, Retrieved 10/09/2017 from VerisCommunity, http://veriscommunity.net/index.html

ThreatConnect (2017, Aug 25), Sharing Threat Intelligence Using STIX-TAXII, Retrieved 15/03/2018 from ThreatConnect, https://threatconnect.com/blog/how-threatconnect-does-stix-taxii/

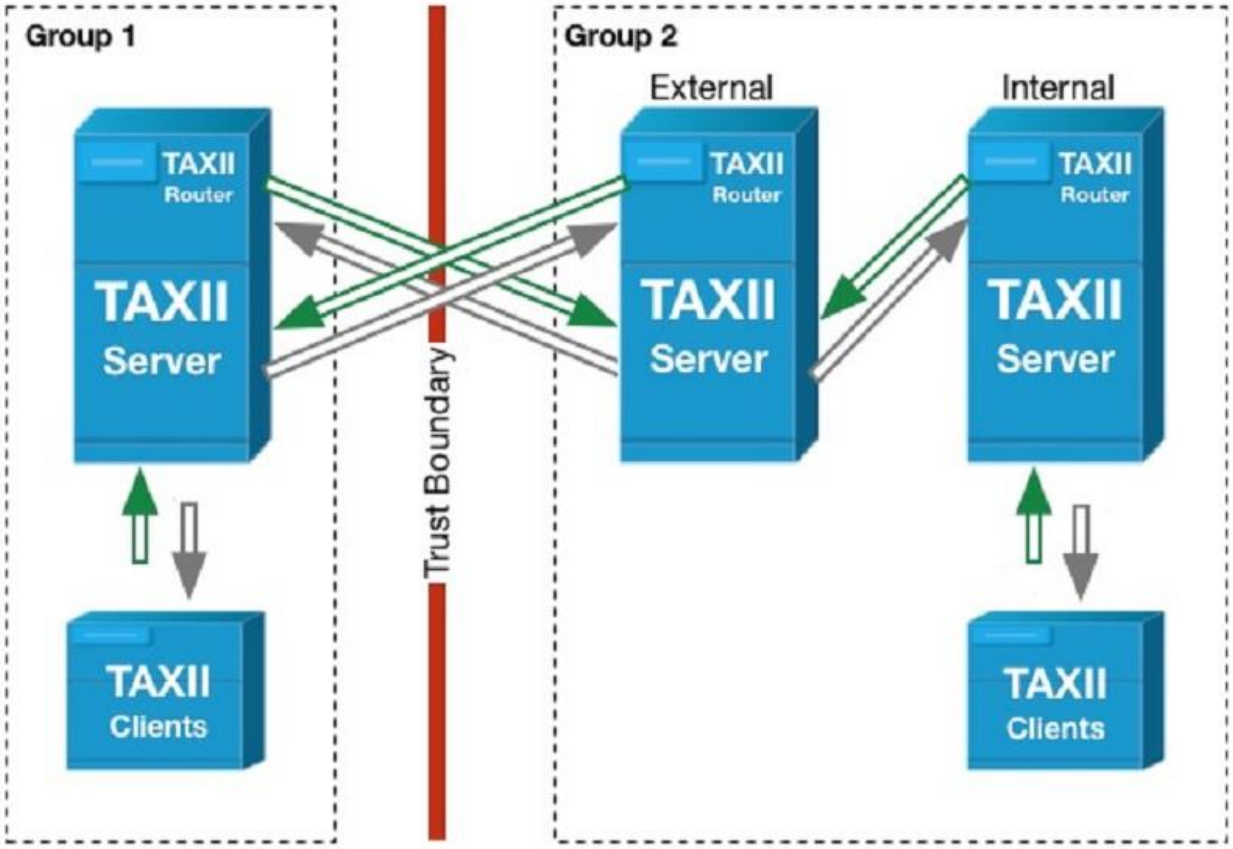
Veerasamy, N. (2017), Cyber threat intelligence exchange: A growing requirement, Retrieved 10/07/2017 from CSIR, https://researchspace.csir.co.za/dspace/bitstream/handle/10204/9462/Veerasamy_19277_2017.pdf?sequence=1&isAllowed=y

Wunder, J. (2017, April 12), CTI Post: STIX 2.0 Finish Line, Retrieved 03/10/2018 from MITRE, https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/stix-20-finish-line

Appendix A: Short description of STIX 2.0 SDOs (1-12) and SROs (13-14)

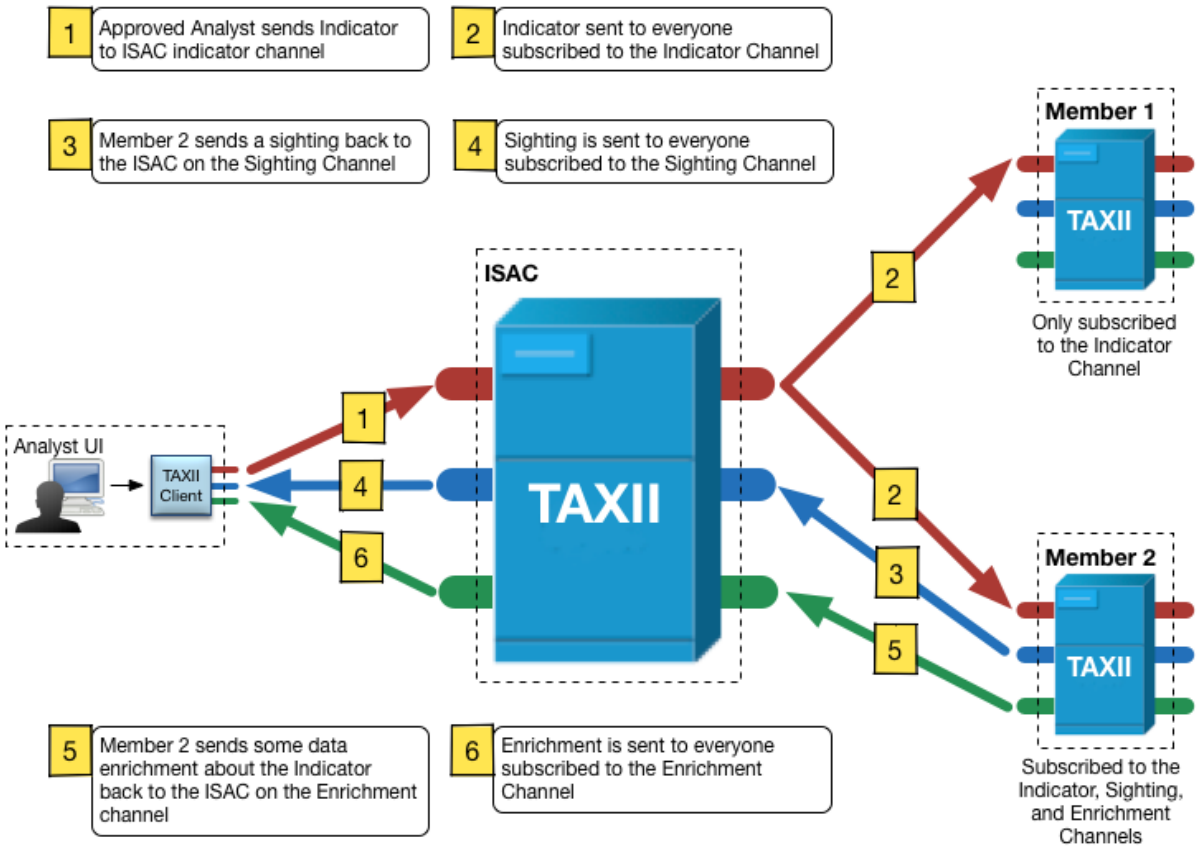
#	Object	Name	Description
1		**Attack Pattern**	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
2		**Campaign**	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
3		**Course of Action**	An action taken to either prevent an attack or respond to an attack.
4		**Identity**	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
5		**Indicator**	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
6		**Intrusion Set**	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
7		**Malware**	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
8		**Observed Data**	Conveys information observed on a system or network (e.g., an IP address).
9		**Report**	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
10		**Threat Actor**	Individuals, groups, or organizations believed to be operating with malicious intent.
11		**Tool**	Legitimate software that can be used by threat actors to perform attacks.
12		**Vulnerability**	A mistake in software that can be directly used by a hacker to gain access to a system or network.
13		**Relationship**	Used to link two SDOs and to describe how they are related to each other.
14		**Sighting**	Denotes the belief that an element of CTI was seen (e.g., indicator, malware).

Appendix B: TAXII 2.0 deployments



Source: https://lists.oasis-open.org/archives/cti-taxii/201509/msg00072.html

Appendix C: TAXII 2.0 channel communication



Source: https://lists.oasis-open.org/archives/cti-taxii/201509/msg00072.html

Appendix D: List of helpful links

OASIS CTI TC Website:

- Home - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

OASIS CTI TC Tools and Approved Publications

- STIX 2.0 Core Concepts - http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html
- STIX 2.0 Objects - http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part2-stix-objects.html
- STIX 2.0 Cyber Observable Core Concepts - http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part3-cyber-observable-core.html
- STIX 2.0 Cyber Observable Objects - http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part4-cyber-observable-objects.html
- STIX 2.0 STIX Patterning - http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html
- TAXII 2.0 - http://docs.oasis-open.org/cti/taxii/v2.0/taxii-v2.0.html
- STIX 2.0 Interoperability Test Document - https://docs.google.com/document/d/1Bk3QsGqS84odU2iJtTZ8GokLZlOuz52iM7QKkRhJtQc/pub
- GitHub STIX2 - https://github.com/oasis-tcs/cti-stix2
- GitHub TAXII2 - https://github.com/oasis-tcs/cti-taxii2

OASIS TC Open Repositories:

- Python APIs for STIX 2 - https://github.com/oasis-open/cti-python-stix2
- Convert STIX 1.2 XML to STIX 2.0 JSON - https://github.com/oasis-open/cti-stix-elevator
- TAXII 2 Server Library Written in Python - https://github.com/oasis-open/cti-taxii-server
- TAXII 2 Client Library Written in Python - https://github.com/oasis-open/cti-taxii-client
- Lightweight visualization for STIX 2.0 objects and relationships - https://github.com/oasis-open/cti-stix-visualization
- GitHub Pages site for STIX, CybOX, and TAXII - https://github.com/oasis-open/cti-documentation
- Non-normative schemas and examples for STIX 2.0 - https://github.com/oasis-open/cti-stix2-json-schemas
- Supports development of a Python application to convert STIX 2.0 content to STIX 1.x content - https://github.com/oasis-open/cti-stix-slider
- Validate patterns used to express CybOX content in STIX Indicators - https://github.com/oasis-open/cti-pattern-validator
- Non-normative schemas and examples for CybOX 3 - https://github.com/oasis-open/cti-cybox3-json-schemas
- Match STIX content against STIX patterns - https://github.com/oasis-open/cti-pattern-matcher
- Validator for STIX 2.0 JSON normative requirements and best practices - https://github.com/oasis-open/cti-stix-validator
- Prototype for processing granular data markings in STIX - https://github.com/oasis-open/cti-marking-prototype

Other Repositories:

- Translate STIX 2 Patterning Queries - https://github.com/mitre/stix2patterns_translator
- Malware Information Sharing Platform & Threat Sharing - https://github.com/MISP/MISP
- A cyber threat intelligence server based on TAXII 2 and written in Golang - https://github.com/freetaxii/freetaxii-server
- APIs for generating STIX 2.x and TAXII 2.x messages with Go (Golang) - https://github.com/freetaxii/libstix2
- The CaRT file format is used to store/transfer malware and its associated metadata - https://bitbucket.org/cse-assemblyline/cart
- Convert STIX2 to GraphML or GEXF (Gephi format) - https://github.com/workingDog/StixConvert
- Convert STIX2 and load into Neo4j graph database - https://github.com/workingDog/StixToNeoDB
- A browser App to add STIX 2.1 objects to a TAXII-2.0 server - https://github.com/workingDog/cyberstation
- STIX2 Scala library - https://github.com/workingDog/scalastix
- TAXII2 Scala library - https://github.com/workingDog/Taxii2LibScala
- TAXII2 JS library - https://github.com/workingDog/taxii2lib
- A repository for development of the TAXII Specifications - https://github.com/TAXIIProject/TAXII-Specifications/wiki